Avaya Call Management System

Security for Linux®

Release 18
February 2018

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

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:

https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"**Hosted Service**" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. " Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "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. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "**Unit**" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole

or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third party components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at:

https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com , or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(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.

Avaya is a registered trademark of Avaya Inc.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com , or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

The purpose of this document is to describe how to implement security features in Avaya Call Management System (CMS) running on the Red Hat Enterprise Linux® (RHEL) operating system.

Intended audience

This document is written for:

- Avaya support personnel.
- Avaya factory personnel.
- Contact center administrators.

Users of this document must be familiar with Avaya CMS and the RHEL operating system.

Related resources

Documentation

See the following documents:

Title	Use this document to:	Audience
Using		
Avaya CMS Administration	Administer CMS.	Implementation engineers and system administrators

Title	Use this document to:	Audience
Avaya CMS LAN Backup User Guide	Learn how to use the LAN backup feature with CMS.	Avaya support personnel, contact center administrators, and Tivoli administrators
Avaya CMS ODBC and JDBC	Learn how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Avaya support personnel and contact center administrators
Implementing		
Avaya CMS Software Installation, Maintenance, and Troubleshooting for Linux®	Install, configure, and maintain Avaya CMS running on the RHEL operating system.	Avaya support personnel, Avaya factory personnel, and contact center administrators

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Documentation changes since last issue

- Added a section to modify crypto ciphers for the web client on the CMS server.
- Updated the release number to CMS R18 across the document.

Documentation Web sites

All CMS documentation can be found at http://support.avaya.com. New issues of CMS documentation will be placed on this website when available.

Use the following websites to view related support documentation:

- Information about Avaya products and services

  http://www.avaya.com
- Dell hardware documentation

  http://www.dell.com/us/enterprise/p/poweredge-r720/pd

Support

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

Chapter 2: Avaya CMS security

This document covers security-related information and configuration settings in the Red Hat Enterprise Linux® (RHEL) operating system and Call Management System (CMS) applications that interest customers. This chapter covers the following topics:

Operating system hardening

The services discussed here may be disabled by customers, business partners, or professional services associates. Avaya provides support for disabling services only if the customer-documented procedures in the administration guide have been followed. Avaya Professional Services also provides a security hardening offer, discussed later, that can upgrade CMS systems to current hardening levels. This results in additional customizable security scripts and features, such as preventing more than one login by a user or an automatic session timeout. The hardening offer is available for CMS systems r3v9 and later. CMS R15 systems must be on load r15ab.d (r15auxab.d) or later. The only R15 load before r15ab.d was r15aa.m or r15auxaa.m. For more information on security features for different versions of CMS, see chapter CMS network security on page 33.

Operating system (OS) hardening can be achieved in the following ways:

Third party security and management packages/tools

Traditionally, viruses do not target Linux®. However, several antivirus and other security software for Linux® are now available. Avaya does not support the use of such software on the CMS product as it can severely impact performance.

The Avaya Permissive Use Support Policy for customers who require third party software to be installed on their CMS system is reproduced in CMS permissive use support policy on page 45.This policy is subject to change in the future releases of CMS.

Log files

There are multiple files in the `/var/log/` directory with numbers after them, for example, `cron-20100906`. These numbers represent a timestamp that gets added to a rotated log file. Log files are rotated so their file sizes do not become too large. The logrotate package contains a `cron` task that automatically rotates log files based on the `/etc/logrotate.conf` configuration file and on the `/etc/logrotate.d/` directory configuration files.

The following sample is from the `/etc/logrotate.conf` configuration file:

```
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# uncomment this if you want your log files compressed
compress
```

All the lines in the sample configuration file define global options that apply to every log file. In this example, log files are rotated weekly, rotated log files are kept for the duration of 4 weeks, and all rotated log files are compressed by gzip into the .gz format. Any lines that begin with a hash sign (#) are comments and the system does not process them.

You can define configuration options for a specific log file and add it under the global options. However, it is advisable to create a separate configuration file for any specific log file in the `/etc/logrotate.d/` directory and define the configuration options there.

The following is an example of a configuration file placed in the `/etc/logrotate.d/` directory:

```
/var/log/messages {
    rotate 5
    weekly
    postrotate
    /usr/bin/killall -HUP syslogd
    endscript
}
```

The configuration options in this file are specific to the `/var/log/messages` log file only. The settings specified here override the global settings where applicable. Thus, the rotated /`var/log/messages` log file will be kept for five weeks instead of four weeks as was defined in the global options.

The following is a list of some of the directives you can specify in your `logrotate` configuration file:

- weekly - Specifies the rotation of log files on a weekly basis. Similar directives include:
  - daily
  - monthly
  - yearly
- compress - Enables compression of rotated log files. Similar directives include:
  - nocompress
  - compresscmd - Specifies the command to be used for compressing.
  - uncompresscmd
  - compressext - Specifies what extension is to be used for compressing.
  - compressoptions - Lets you specify any options that can be passed to the used compression program.
  - delaycompress - Postpones the compression of log files to the next rotation of log files.
- rotate <INTEGER> - Specifies the number of rotations a log file undergoes before it is removed or mailed to a specific address. If you specify the value 0, old log files are removed instead of rotated.
- mail <ADDRESS> - This option enables mailing of log files that have been rotated as many times as is defined by the rotate directive to the specified address. Similar directives include:
  - nomail
  - mailfirst - Specifies that the system must mail the just-rotated log files, instead of the about-to-expire log files.
  - maillast - Specifies that the system must mail the about-to-expire log files, instead of the just-rotated log files. This is the default option when mail is enabled.

For the full list of directives and various configuration options, refer to the `logrotate` man page. Use command *man logrotate*.

System auditing

The system stores various audit events in the `/var/log/audit/audit.log` file.

The Audit system operates on a set of rules that define what to capture in the log files. You can specify three types of Audit rules:

- Control rules: Using control roles, you can modify the Audit system's behavior and some of its configuration.
- File system rules: Using file system rules, which are also known as file watches, you can audit access to a particular file or a directory.
- System call rules: Using system call rules, you can log system calls that any specified program makes.

You can specify audit rules on the command line with the `auditctl` utility but these rules are not persistent across reboots. You can also write audit rules in the `/etc/audit/audit.rules` file.

Using the `auditctl` command, you can control the basic functionality of the Audit system and define rules that decide which Audit events are logged.

About defining Control Rules

Use the prefixes of `auditctl` to define control rules to modify the behavior of the Audit system:

Command	Description
`# auditctl -b 8192`	Sets the maximum amount of existing Audit buffers in the kernel.
`# auditctl -f 2`	Sets the action that is performed when a critical error is detected.The above configuration triggers a kernel panic in case of a critical error.
`# auditctl -e 2`	Enables and disables the Audit system or locks its configuration. The above command locks the Audit configuration.
`# auditctl -r 0`	Sets the rate of generated messages per second. The above configuration sets no rate limit on generated messages.
`# auditctl -s`	Reports the status of the Audit system. Output of this command: `AUDIT_STATUS: enabled=1 flag=2 pid=0 rate_limit=0 backlog_limit=8192 lost=259 backlog=0`

Command	Description

`# auditctl -l`	Lists all currently loaded Audit rules.
	Output of this command:
	`LIST_RULES: exit,always watch=/etc/localtime perm=wa key=time-change`
	`LIST_RULES: exit,always watch=/etc/group perm=wa key=identity`
	`LIST_RULES: exit,always watch=/etc/passwd perm=wa key=identity`
	`LIST_RULES: exit,always watch=/etc/gshadow perm=wa key=identity`

`# auditctl -D`	Deletes all currently loaded Audit rules. Output of this command: `No rules`

About defining File System rules

To define a file system rule, use the following syntax:

`auditctl -w path_to_file -p permissions -k key_name`

where:

- *path_to_file* is the file or directory that is audited
- *permissions* are the permissions that are logged
  - r - read access to a file or a directory
  - w - write access to a file or a directory
  - x - execute access to a file or a directory
  - a - change in the attribute of the file or directory
- *key_name* is an optional string that helps you identify which rule or a set of rules generated a particular log entry.

About defining System Call rules

To define a system call rule, use the following syntax:

`auditctl -a action,filter -S system_call -F field=value -k key_name`

where:

- *action* and *filter* specify when a certain event is logged. *action* can be either **always** or **never**. *filter* specifies which rule-matching filter of the kernel is applied to the event. The rule-matching filter can be one of **task**, **exit**, **user**, or **exclude**.

- *system_call* specifies the system call by its name. You can find a list of all system calls in the `/usr/include/asm/unistd_64.h` file. You can group several system calls into one rule, each specified after the -S option.
- *field=value* specifies additional options that further modify the rule to match events based on a specified architecture, group ID, process ID, or other parameters. For a full listing of all available field types and their values, refer to the `auditctl(8)` man page.
- *key_name* is an optional string that identifies which rule or set of rules generated a particular log entry.

About persisting Audit Rules across reboots

For Audit Rules to persist across reboots, they must be included in the `/etc/audit/audit.rules` file. They must be entered using the same argument syntax that are used with the `auditctl` program.

For example, the following `audit.rules` file includes a File System rule to log all writes and attribute changes of the /etc/passwd file:

```
# This file contains the auditctl rules that are loaded
# whenever the audit daemon is started via the initscripts.
# The rules are simply the parameters that would be passed
# to auditctl.

# First rule - delete all
-D

# Increase the buffers to survive stress events.
# Make this bigger for busy systems
-b 320

# Feel free to add below this line. See auditctl man page
-w /etc/passwd -p wa -k passwd_changes
```

Please reference the man pages for `auditd`, `auditctl`, and `audit.rules` for detailed information about available auditing/logging options.

Reading/Searching Audit Logs

The **ausearch** program is used to search the audit logs without having to decipher the formatting used in the `audit.log` file. Refer to the **ausearch** man page for a detailed description of the available options.

To search for failed login attempts, use the following command:

```
# ausearch --message USER_LOGIN --success no --interpret
```

To search for all logged actions performed by a certain user, using the user's login ID, `auid`, use the following command:

```
# ausearch -au 500 -i
```

To search for all failed system calls from yesterday up until now, use the following command:

```
# ausearch --start yesterday --end now -m SYSCALL -sv no -i
```

More Information

For more information about the Audit system, refer to the following sources:

- Online Sources
  - The Linux Audit system project page http://people.redhat.com/sgrubb/audit/.
  - Article Investigating kernel Return Codes with the Linux Audit System in the *Hack In the Box* magazine:

    http://magazine.hackinthebox.org/issues/HITB-Ezine-Issue-005.pdf.
- Installed Documentation

  Documentation provided by the audit package can be found in the /usr/share/doc/audit-version/ directory.
- Manual Pages
  - audispd.conf(5)
  - auditd.conf(5)
  - ausearch-expression(5)
  - audit.rules(7)
  - audispd(8)
  - auditctl(8)
  - auditd(8)
  - aulast(8)
  - aulastlog(8)
  - aureport(8)
  - ausearch(8)
  - ausyscall(8)
  - autrace(8)

Patching and patch qualification

Avaya continuously monitors security alerts from a variety of sources, analyzes potential product impact, and posts appropriate product advisories at the Avaya Product Security Support web site, http://support.avaya.com/security. Customers may register at this web site to receive automatic notification of new and updated security advisories.

Avaya Labs conducts research and participates in international activities of security bodies, creating best practices for product development groups. Products are measured against such best practices, and improvements regularly made based on these assessments.

CMS includes all necessary components including security patches at the time of release. Avaya receives additional patch notifications from various sources and certifies new Linux® OS patches and RPMs. Then, Avaya assembles the patch clusters and makes these available to customers. Avaya also updates security advisories with instructions on downloading and applying these certified patches when they are made available on the Avaya support Web site. Installation of patches is a customer responsibility unless specified otherwise in a premium services contract. Customers should contact services if they have questions regarding a specific patch.

Only the Avaya approved Linux® patches and RPMs should be installed. All patches and RPMs are not required or fit for use on the CMS system as it does not incorporate all aspects of RHEL. Installing Linux® patches or RPMs not recommended by Avaya can cause problems with the CMS server.

Note:

Avaya approves installation of kernel patches through the baseload or version upgrade process. The kernel patches are not released through any other method.

Altering the ssh, telnet and ftp network service banners

Altering the telnet and ftp network service banners hides operating system information from individuals who want to take advantage of known operating system security holes.

To alter the telnet and ftp network service banners:

1. Create or edit the file `/etc/issue.net`.
2. Add the line:

   `"CMS OS"`

3. Save the file.
4. Change the file permissions to 444.

Banner modifications

Note:
The system displays banner messages only when you use interactive terminal sessions. These messages are not displayed in CMS Supervisor PC client or CMS Supervisor Web.

You can modify the banners displayed on login to any CMS system to obscure OS or application information or display legal access warnings.

Displaying a restricted warning for telnet users performs the following functions:

- Displays your corporate policy for illegal computer activity
- Scares off some individuals who might want to access a system illegally
- Allows you to prosecute an individual who has illegally accessed the system

To display a restricted warning for telnet users:

1. Create or edit the following files:
   - `/etc/issue.net` : The system displays the banner prior to the user logging in.
   - `/etc/motd` : The system displays the banner after the user is authenticated.

   ```
   # telnet cms_box
   Trying 192.168.1.22...
   Connected to cms_box.
   Escape character is '^]'.
   CMS OS
   ```
2. Add a message similar to the following:

   ```
   WARNING: This system is restricted to Company Name authorized users for
   business purposes. Unauthorized access is a violation of the law. This system
   may be monitored for administrative and security reasons. By proceeding, you
   consent to this monitoring.
   ```

   When users connect to the Avaya CMS system using network services, the system displays the warning message. A user would see the message if they telnet into the Avaya CMS system.
3. Save the file.
4. Change the file permissions to 644.

E-mail and SMTP

You should not configure CMS as a mail relay and not enable the Simple Mail Transfer Protocol (SMTP) daemon.

DNS and NFS

In general, there is no support for sharing file systems to and from CMS system and you should disable associated daemons on older CMS systems. If `hosts.allow` and `hosts.deny` (or `.rhosts`) files are used for access control, any servers or files that control name resolution (Domain Name Servers or entries in the `/etc/hosts` file) are under appropriate administrative control within the customer network. This prevents an attacker from leveraging DNS services to enter a system.

User file permissions and masks

Due to limitations in the CMS system, a umask value of up to 0022 can be supported without impacting product functionality.

Authentication and session encryption

This section covers the following topics:

User authentication and authorization

CMS uses login and password security measures within the RHEL OS and provides multiple levels of system access. To authenticate users, CMS uses RHEL capabilities, based on Pluggable Authentication Modules (PAM). At the system level, standard UNIX permissions are used. Within CMS, data permissions are administered per user.

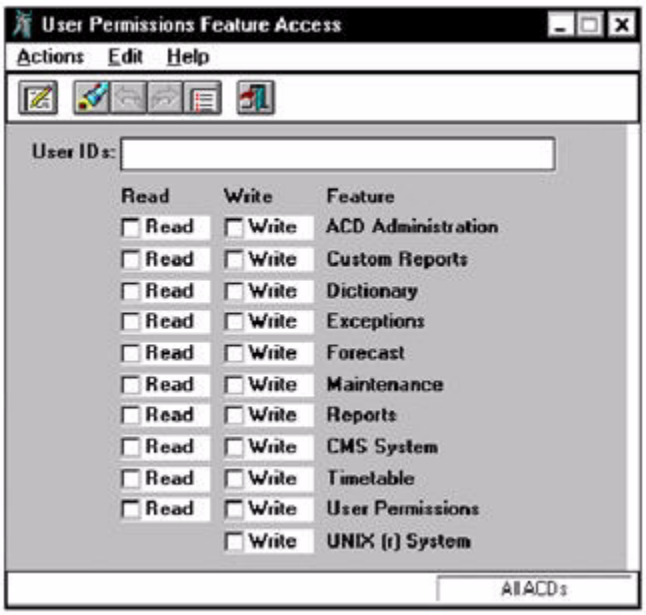
When you create a user in Call Management System, you provide the user either administrator or user access rights. As an administrator, your ability to modify the configuration of a CMS server is limited to the feature permissions provided to you. CMS user accounts are not permitted to make administrative changes unless they have been given the required feature permissions. Ordinary CMS users are not provided OS privileges and can be limited within the application, to particular skills, VDN, and trunk groups. Avaya also implements feature controls that must be unlocked in order to access the feature.

Using PAM configuration files, RHEL allows for integration with external authentication within a UNIX domain using a Network Integration Service (NIS or NIS+). CMS does not support add-on authentication packages for other external authentication services for RHEL. Use of external authentication may bypass local rules configured for password expiration and complexity, such as the settings within the two OS files /etc/passwd and /etc/shadow.

Avaya Access Security Gateway (ASG) software can authenticate Avaya Services and other remote users. This mechanism supports a one-time password. The system presents the user with a challenge string to which they respond with a string generated by a software tool, based on the challenge and product identification information.

You can define the following access permissions for each user login and password in CMS:

- ACD Access: User can assign, view, delete, and modify another user's ability to gain access to one or more real or pseudo ACDs. You can also turn on or off the exceptions notification for ACDs in this window.
- Feature Access: User can assign, view, or modify user access permissions for the CMS subsystems such as Reports, Dictionary and Exceptions and certain function key (SLK) menu items, such as UNIX system/RHEL system and Timetable. The access permissions given to a user affect what that user is able to do with CMS.



- Main Menu Addition Access - User can assign, view, or modify other users' access permissions for the additional menu items of your choosing. These items could be access to your local electronic mail environment or daily news articles about your call center for agents or split/skill supervisors.
- Split/Skill Access - User can assign, view, modify, or delete another user's permissions to specific splits/skills. Split/Skill Access permissions determine your ability to access and administer agent/queue data for a particular split or skill. You must also turn on or off the exceptions notification for splits/skills in this window.
- Trunk Group Access - User can assign, view, modify, or delete another user's access permissions to specific trunk groups. Trunk Group Access permissions determine a user's ability to access and administer data for a particular trunk group. You must also turn on or off the exceptions notification for trunk groups in this window.
- User Data - User can assign CMS user IDs, specify a default printer,specify whether the user is an administrator, or a normal user such as a splits/skill supervisor, and administer the maximum number of open windows, the minimum refresh rate for real-time reports, and the default login ACD.
- VDN Access - User can assign, view, modify, or delete another CMS user's access permissions to specific VDNs. VDN access permissions determine a user's ability to administer VDNs with the various CMS subsystems and to access report/administration data for VDNs.
- Vector Access - User can define vector access permissions. These permissions specify the user's ability to administer vectors and to access report/administration data for vectors. Use to assign, view, modify, or delete a CMS user's access permissions to specific vectors.

Password complexity and expiration

In CMS, you can enable and modify the password expiration attributes through the CMSADM menu. You can set the expiration intervals from 1 to 52 weeks. For detailed instructions for configuring aging, see Enabling password aging on page 22.

Some custom integrations and configurations with scripted passwords may require careful application of password expiration settings. For this, you should always use the CMSADM script. Avaya does not recommend direct administration of password aging through RHEL.

Enabling password aging

Password aging forces users to change their passwords on a regular basis.

Using passwd_age

Use the `passwd_age` option to turn password aging on or off. If password aging is on, users will be prompted to enter a new password after a predetermined time interval has passed. Password aging is off by default.

CAUTION:
If you have any third party software or Avaya Professional Services (APS) offers, do not turn on password aging. Contact the National Customer Care Center (1-800-242-2121) or consult with your product distributor or representative to ensure that password aging will not disrupt any additional applications.

The `passwd_age` option will effect the passwords of all Avaya CMS users and regular UNIX users. When password aging is on, the RHEL policy file `/etc/default/passwd` is modified. The passwords of all Avaya CMS users that use the `/usr/bin/cms` shell and all UNIX users will age. If password aging is on when a new user is added, the user's password begins to age as soon as a password is entered for that account. It is recommended that you exclude specific users before turning password aging on in order to avoid additional password administration. If you need to prevent the aging of a specific user's password, see Adding and removing users from password aging and Troubleshooting password aging sections in *Avaya CMS Software Installation, Maintenance and Troubleshooting*.

Important:
Non-CMS users such as `root`, `root2`, or `informix` will not age. Password aging will not function on an Avaya CMS system that uses a NIS, NIS+, or LDAP directory service. If you are using NIS, NIS+, or LDAP, contact your network administrator. The passwords will need to be aged from the server running the directory service.

To use the `passwd_age` option:

1. Enter:

   `cmsadm`

   The system displays the CMSADM menu.

2. Select number for “passwd_age” menu item.

   The system displays the following message:

Note:
The system will also display a message that indicates that password aging is off or the current password aging schedule. You may enter q at any point to exit the password aging options.

3. Perform one of the following actions:

- To turn password aging on:

a. Enter: 1

The system displays the following message:

b. Enter the number of weeks before passwords expire and users are prompted to enter a new password. The range is from 1 to 52 weeks.

- To turn password aging off:

  a. Enter: 2

  The system displays the following message:

  b. Perform one of the following actions:

     – To turn password aging off, enter: yes
     – To leave password aging on, enter: no

- To change the password aging interval:

  a. Enter: 3

  The system displays the following message:

  b. Enter the number of weeks before passwords expire and users are prompted to enter a new password. The range is from 1 to 52 weeks.

RHEL password complexity rules and considerations

The password complexity requirements for CMS R18 are based on a standard RHEL methodology using pluggable authentication modules (PAM). The rules are specified in the `/etc/pam.d/system-auth` file.

The default version of this file is shown here:

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth required pam_env.so
auth sufficient pam_fprintd.so
auth sufficient pam_unix.so nullok try_first_pass
auth requisite pam_succeed_if.so uid >= 500 quiet
auth required pam_deny.so
account required pam_unix.so
account sufficient pam_localuser.so
account sufficient pam_succeed_if.so uid < 500 quiet
account required pam_permit.so
password requisite pam_cracklib.so try_first_pass debug retry=3 type=
password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password required pam_deny.so
session optional pam_keyinit.so revoke
session required pam_limits.so
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required pam_unix.so
```

There are four sections in this file. The `auth` rules apply to authentication. The account rules verify that access to an account access is allowed by making sure that the account is not locked or expired. The password rules process password alteration and the complexity of those passwords. The session rules configure the user sessions. For example, the session rules determine if the home directory of the user is mounted or not.

The system processes the rules in order. Consider the password rules which process password complexity. The *requisite* parameter means that the password rule must succeed in order to continue. If the PAM module, `pam_cracklib`, passes, the rule moves to the `pam_unix` module. The password for `pam_unix` comes from `pam_cracklib`. The arguments accompanying `pam_unix` allow the password to be passed to `pam_unix` from `pam_cracklib` without prompting for another password. SHA512 specifies that this algorithm should be used to encrypt the password and that the system should maintain the /etc/shadow file. This module also processes all the shadow elements which include expiration, last change, max change, min change, and warn change. Assuming that these aging conditions are met, the module is considered sufficient and the system allows the log in. If this rule fails, the rule moves to the next module, `pam_deny`, which denies the log in.

pam_cracklib

This is the main module responsible for enforcing good passwords. The default behavior of this module is as follows:

- Deny if the password is part of a dictionary word. The default dictionary is located in `/usr/share/dict/words` and contains almost 500,000 words.
- Deny if the password is a palindrome.
- Deny if the password is simply a change in case of the old one.

- Deny the password if it is similar to the old one.
  - By default, the number of characters that must change is the smaller of 10, or half the length of the new password. You can modify this behaviour using the **difok** parameter
  - By default, characters after the 23rd character are ignored for the purpose of this calculation. You can modify this behaviour with the **difignore** parameter.
- Deny the password if it is simple.
  - This is a length check that is controlled by the following parameters:
    - minlen
    - maxclassrepeat
    - dcredit
    - ucredit
    - lcredit
    - ocredit
- Deny if the password is a rotated version of the old one.
- Deny if the password has too many consecutive characters. This is defined by the **maxrepeat** parameter.
- Deny if the password contains username in some form. This is defined by the **reject_username** parameter.
- Deny if the password does not contain at least one upper case character.
- Deny if the password does not contain at least one numeric character.

Problems with SHA512 passwords

Since CMS R18 uses SHA512 passwords instead of standard Unix crypt passwords which are used in Solaris, passwords can be longer than 8 characters. This can cause a problem with `pam_cracklib` and the default complexity rules.

For example, It can be difficult to change the password *ThisIsMyPasswordAndILoveIt* under the default conditions because 10 of these characters must change or not be present in the new password. As a result, the longer and more complex the passwords get, the more difficult it is to change them to something that will meet the complexity criteria. This can be worked around by modifying the **difok** and **difignore** parameters to the `pam_cracklib` module.

It is important to understand what the `pam_cracklib` and `pam_unix` PAM modules do and what parameters can be changed. Detailed descriptions of these arguments can be found in the man pages for `pam_cracklib` and `pam_unix`.

WARNING:
Great care should be taken when changing arguments to the PAM modules. If there is a mistake, the system can deny a log in. Esure backing up any files before making changes. For more information, see the man pages for `pam_cracklib` and `pam_unix`.

Session timeouts and multiple-login prevention

By default, no timeouts exist for agent or administrator login sessions on the CMS system. However, you can configure a cron job for this purpose. Avaya also offers a custom hardening service that you can use to create an equivalent function. In addition, the CSI hardening offer prevents a login from being used more than once concurrently.

See more details on this hardening offer in CMS security/Hardening offer on page 49.

FIPS considerations

CMS provides the option to turn on FIPS 140-2 compliant mode for the following:

- ssh communications used by the CMS PC client.
- https communications used by the CMS web client.

CMS does not adopt FIPS 140-2 encryption for other connections, such as the CMS/CM spi link, ODBC/JDBC connections, external call history data transfer (ECHI APS offer), and CMS HA synchronizations (HA-AdminSync APS offer).

You must enhance the cmssvc menu to include a security option to allow users to enable or disable the FIPS 140-2 mode for CMS ssh and https connections. For more information on the cmssvc menu, see *Avaya Call Management System Software Installation, Maintenance, and Troubleshooting for Linux®*.

Standard UNIX one-way password encryption is used within the `/etc/shadow` file.

Use of telnet, ftp, tftp, rsh

Traditionally, computer-based CMS clients, such as Supervisor, Terminal Emulator, and Network Reporting, use `telnet` to interface with the CMS server. Avaya discourages the use of `telnet` for communication over a network because it is an insecure protocol. For example, in `telnet`, passwords are exchanged in clear text.

Therefore, users logging in to the CMS server must use `ssh` for server connections. In the case of `tftp` and `rsh`, these protocols are unauthenticated or easily spoofed. To avoid this, use secure equivalents such as `scp` and `sftp`.

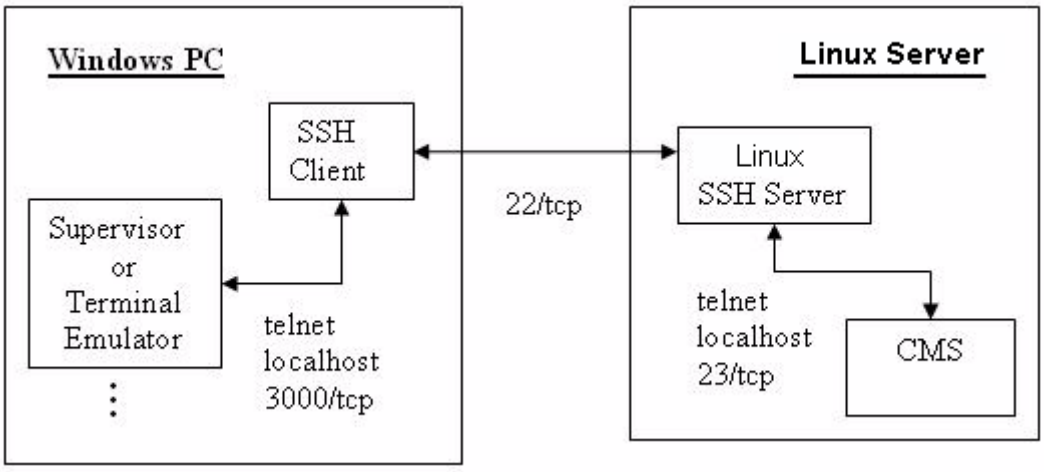
To limit interactive access, you should always provision ordinary users with the `/usr/bin/cms` shell.

Using ssh within CMS

Use Secure Shell (`ssh`), a protocol that encrypts the packets sent between a client workstation and a host server. This secures the transmission of login information and other sensitive data.

On the client, an SSH client package creates the SSH tunnel and does the encryption/decryption for the SSH connection. In addition, the Microsoft Crypto API provides the password encryption and decryption functionality. It protects the login/password information stored in the registry for automatic scripts.

The following figure illustrates the connectivity between the various components:



On the CMS server, you can restrict the telnet service to the local host using the following restrictions:

- `/etc/hosts.allow`

  `in.telnetd : localhost` # allow telnet only from within the server
- `/etc/hosts.deny`

  `in.telnetd`: ALL # deny all telnet except as specified in hosts.allow

Other points to be noted:

- Although the telnet service runs on the CMS server, it is configured so that any attempt to gain access to port 23 from outside the system results in a "connection refused" message.

- In CMS, the Windows SSH clients and SSH server negotiate the encryption algorithm, typically 128-bit AES (recommended) or Blowfish. A variety of industry standard algorithms, such as 128-bit AES, Blowfish, SHA-1, MD5, RC4, and key lengths are provided as a result of including an SSH client. The specific algorithm is negotiated between the client and the server. The U.S. government accepts all for domestic and international use, with certain restrictions. Selection of an algorithm takes place at run time. SSH uses RSA or DSA. CMS servers use SSH Protocol 2. The default encryption method for RHEL is SHA512. See the `/etc/login.defs` file.

CMS application security

This section covers the following topics:

SPI link

The SPI link is a binary (not text-based), proprietary protocol used to communicate between the CMS system and the Communication Manager ACD switch. Access can be controlled by IP address. Communication Manager sends ACD configuration information and ACD-related events to the CMS using this communication channel. For instance, CMS systems can use the SPI link to modify CM vectors, agent and VDN assignments.

Application-level audit logging

There are several application logs with CMS. The most detailed application audit trails can be traced through the `/cms/install/logdir/admin.log` and the `/cms/pbx/acd?/spi.err` logs. The `admin.log` records administrative changes to the CMS application. The `spi.err` logs show the information for setting up and debugging ACD links. These logs are intended for support purposes, but can provide a partial audit trail for customers.

CMS also provides the log `/opt/cc/ahl/log`. This log tracks changes to specific system files that affect the administration of the RHEL system. For example, changes to `/etc/hosts` are logged in the `ahl` log.

Avaya COMPAS Document ID 90815 (R3V11 CMS Maintenance Logs Guide) provides detailed information regarding these log files, their formats and messages.

The customer error log is accessible from the main CMS menu ("Error log report" under the maintenance menu).This log was designed to be the primary customer-facing application log, but does not capture the debug and trace information included in other logs, such as admin.log and spi.err.

Backup and restore support

CMS supports direct backup to a tape system, NFS, and several LAN backup solutions. For more information, see *Avaya CMS Software Installation, Maintenance, and Troubleshooting*.

Database security controls

CMS users do not log in to the Informix database or have any privileges within the Informix subsystem. High-level users and administrators can use the `dbaccess` utility on CMS for accessing data. However, ordinary users can gain access to the database only through the CMS application using the access controls provided by CMS. An ISQL interface is installed on the CMS systems. This is an internal password-protected interface that does not have an external or network-facing listener. The user access to the database is provided only through inter-process communication (IPC), so an external exposure to the CMS database is limited to the these interfaces unless the user uses ODBC/JDBC. The ODBC/JDBC interface requires a password for all client connections. For more information, see *Avaya CMS ODBC and JDBC*.

Physical Security

The Avaya CMS system should be installed in an area restricted to persons of trust, such as a locked server room or data center. This section covers the following topics:

Physical server protection

The keyboard, console, CD-ROM, and tape drive are all sensitive devices and may be used to compromise an unprotected CMS system.

Store all backup tapes and all original Avaya CMS software in a secure location on site. Avaya recommends that a copy of the backup tapes be stored at an off site location to aid disaster recovery.

Avaya CMS systems can be configured to use Access Security Gateway (ASG) or SAL to provide secure remote access.

EEPROM / BIOS security

Dell servers provide a BIOS level security mechanism for controlling access to the console. The server provides this by restricting BIOS access to users by making use of a password to enter BIOS settings or before booting. For support purposes, Avaya recommends that customers consider other methods since a forgotten password can require hardware replacement.

Services security and CMS support

This section covers the following topics:

Remote connectivity and authentication

CMS supports the Access Security Guard (ASG) software or ASG guard hardware to provide a one-time, challenge-response authentication for remote access. CMS also supports SAL for secure remote access. Contact your Avaya Services representative for options and details.

Services password management

Avaya Services can automatically change services passwords for the CMS system under an active maintenance contract. Contact your Avaya Services representative for details on how to enable this service.

Adding a firewall

Add a firewall on the edge of the network where the Avaya CMS system and Avaya CMS Supervisor clients reside. Avaya recommends that both the Avaya CMS system and Avaya CMS Supervisor clients remain behind a firewall to provide protection from the internet.

Firewalls are commonly used to prevent denial of service attacks on application servers similar to the Avaya CMS system. Firewalls will also prevent snooping of sensitive data, and hijacked sessions from appearing as an authenticated user.

On Linux, the firewall is managed through the iptables and ip6tables services. CMS provides a utility to generate the firewall rules and to start and stop the firewall services.The utility is also included in the new security option for cmssvc menu. For more information to turn on or off the firewall, see *Avaya Call Management System Software Installation, Maintenance, and Troubleshooting for Linux*®.

Transmitting passwords

Do not use telnet or ftp to transmit passwords over the network in clear text. If you do so, the password can be snooped in transit.

Chapter 3: CMS network security

This chapter discusses how the Red Hat Enterprise Linux® (RHEL) networking component helps to implement the various security features in CMS.

Limiting external access to UNIX services

The CMS security script run during installation creates the files `/etc/hosts.allow` and `/etc/hosts.deny`. Use these files to control which IP addresses are permitted to connect to the Avaya CMS system. Note that settings in `/etc/hosts.allow` cannot re-enable any services disabled through other means.

Note:
`/etc/hosts.allow` and `/etc/hosts.deny` are only honored when TCPWRAPPERS are enabled (which they are by default).

For example, you may want to:

- Deny telnet access to IP addresses outside the company firewall
- Permit SSH connections from IP addresses outside the company firewall
- Only permit SSH connections.

Detailed instructions for modifying services configuration files are found in Controlling who can connect to the CMS system on page 39.

Limiting root access

Disabling root SSH logins

To prevent root logins using the SSH protocol, edit the configuration file of the SSH daemon, `/etc/ssh/sshd_config`, and change the line that reads:

```
#PermitRootLogin yes
```

to

```
#PermitRootLogin no
```

This change has the following effects:

- It prevents root access using the OpenSSH suite of tools. The following programs are prevented from accessing the root account:
  - ssh
  - scp
  - sftp

This change does not affect programs that are not part of the OpenSSH suite of tools.

Using Pluggable Authentication Module to limit root access to services

Pluggable Authentication Module (PAM) uses the /lib/security/pam_listfile.so module for providing flexibility in denying specific accounts. The administrator can use this module to reference a list of users who are not allowed to log in. To limit root access to a system service, edit the file for the target service in the /etc/pam.d/ directory and ensure that you aunthenticate the service by using the pam_listfile.so module.

The following example demonstrates how the module entry appears in the /etc/pam.d/vsftpd PAM configuration file for the vsftpd FTP server. The \ character at the end of the first line is not necessary if the directive is on a single line.

```
auth   required   /lib/security/pam_listfile.so   item=user \
sense=deny file=/etc/vsftpd.ftpusers onerr=succeed
```

This instructs PAM to consult the /etc/vsftpd.ftpusers file and deny access to the service for any listed user. The administrator can change the name of this file, can keep separate lists for each service, or use one central list to deny access to multiple services.

If the administrator wants to deny access to multiple services, you can add a similar line to the PAM configuration files such as /etc/pam.d/pop and /etc/pam.d/imap for mail clients, or /etc/pam.d/ssh for SSH clients.

Using PAM has the following effects:

- It prevents root access to network services that make use of PAM. The following services are prevented from accessing the root account:
  - login
  - gdm
  - kdm
  - xdm
  - ssh

- scp
- sftp
- FTP clients
- Email clients
- Any PAM aware services

PAM has no effect on programs and services that are not PAM aware.

Network Services

Network services can pose many risks for Linux® systems. Some of the primary issues are as follows:

- *Denial of Service attacks (DoS) :* By flooding a service with requests, a Denial of Service attack can bring a system to a halt as it tries to log and answer each request.
- *Script Vulnerability Attacks :* If servers like Web servers are using scripts to execute server-side actions, a cracker can mount an attack on improperly written scripts. These script vulnerability attacks can lead to a buffer overflow condition or allow the attacker to alter files on the system.
- *Buffer Overflow Attacks :* Services which connect to ports numbered 0 through 1023 must run with the user login of the administrator. If the application has an exploitable buffer overflow, an attacker could gain access to the system as the user running the daemon. As a result of exploitable buffer overflows, crackers use automated tools to identify systems with vulnerabilities. Once they gain access, they use automated rootkits to maintain access to the system.

To enhance security, most network services installed with RHEL are turned off by default. Some notable exceptions are:

- `cupsd` : The default print server for RHEL.
- `lpd` : An alternate print server.
- `xinetd` : A super server that controls connections to a host of subordinate servers, such as `vsftpd` and `telnet`.
- `sendmail` : The `Sendmail` mail transport agent is enabled by default, but only listens for connections from the localhost.
- `sshd` : The `OpenSSH` server, which is a secure replacement for `Telnet`.

Leave these services running only if the resources controlled by these services are available. For example, if a printer is not available, do not leave `cupsd` running. If you do not mount NFSv3 volumes or use `ypbindservice` for NIS, then disable `portmap`.

RHEL ships with three programs designed to switch services on or off. They are the **Services Configuration Tool** called `system-config-services`, `ntsysv`, and `chkconfig`. See the man pages of these commands for usage information.

Linux® services that can be disabled

On CMS systems prior to R12, the network services listed below are *not* required for standard CMS operations and can be disabled. For CMS systems R12 and later, these unnecessary services have been disabled by default. Note that custom scripts or other custom integration added after installation as part of an Avaya Professional Services Offer may require one or more of these services. The following network services are allowed to be disabled when not required for customized integration:

- `Chargen` (19/tcp, 19/udp)
- `Daytime` (13/tcp, 13/udp)
- `Discard` (9/tcp, 9/udp)
- `Echo` (network echo - 7/tcp, 7/udp)
- `Finger` (79/tcp)
- `FTP` (inbound - 21/tcp)
- `Kerberos V5 Warning Message Daemon` (88/tcp, 88/udp)
- `Name` (42/udp)
- `NFS Server` (2049/tcp, 2049/udp)
- `NFS Client` (lockd - 4045/tcp, 4045/udp)
- `NIS Client`
- `Printer` (Network printing services, local printing is enabled - 515/tcp)
- `Rexec` (512/tcp)
- `Syslog` (514/udp)
- `Rsh` (514/tcp)
- `Rlogin` (513/tcp)
- `Sendmail` (inbound - 25/tcp)
- `Spray` (100012/tcp, 100012/udp)
- `Font Server` (7100/tcp)
- `Talk` (517/tcp)
- `UUCP Network services` (540/tcp)
- `Time Service` (37/tcp, 37/udp)
- `Wall`

Disabling some of these services may interfere with network-related troubleshooting activities such as `echo`, and network monitoring tools.

`Telnet` (23/tcp) cannot be disabled even if `ssh` has been configured for clients, but it can be restricted to the local host so that it does not respond externally.

Firewall traversal considerations / Open ports

The CMS system can be placed behind a packet filtering firewall, although no support for such configurations is provided (especially when Network Address Translation (NAT) takes place). Please see below for a list of port requirements for various aspects of CMS operations. Note that many CMS systems receive additional customization and configuration that may add to this list or make some optional items mandatory.

Also note that ports administered for the ACDs can be changed

- 22/tcp ssh (optional, can be used by Supervisor, clients)
- 23/tcp telnet (used by Supervisor; optional for Terminal Emulator)

Optional ports:

- 21/tcp: ftp, used by a CSI (customized configuration) offer
- 25/smtp: sendmail, used by a CSI offer and SAL Gateway
- 37/tcp time: used by a CSI offer
- 123/udp NTP: used by SAL Gateway
- 161/udp, 162/udp: SAL Gateway
- 443/tcp: SAL Gateway
- 514/tcp: rsh, used by the High Availability option for the admin-sync utility (CSI offer). Also required for remote tape copy (provisioning)
- 540/tcp: uucp, used by the External Call History (ECH) interface
- 631/tcp: Internet Printing Protocol
- 705/tcp: SAL Gateway, SNMP
- 725/tcp: SNMP
- 3077/tcp, 3078/tcp: HA Admin Sync
- 3889/tcp: SAL Gateway
- 4046/tcp: NFS
- 9100/tcp, udp: hp-printers
- 515/tcp, udp: Printer server
- 6060: Geotel

- 9999: CVLan
- 9980: Link Admin
- 5678: Definity LAN Gateway
- 5011/5012: ASAI
- 5160/tcp: SNMP
- 6001/tcp: X11
- 5107/tcp, 5108/tcp: SAL Gateway
- 7443/tcp: SAL Gateway
- 8000/tcp: SAL Gateway
- 8089/tcp, Apache Tomcat: used by CMS Web Client
- 8080/tcp, 8443/tcp: CMS Web Client
- 111/tcp/udp rpcbind (used by CDE)
- 50000/tcp, 50001/tcp: Informix ODBC/JDBC
- 32771-32772/tcp and udp: Used by NFS status daemon (necessary if NFS backup is being used).

Note:

Many processes and applications open private ports in the range of 49152 to 65535 as temporary communication channels. The system can have a number of ports in this range open. In order to determine which CMS process is using a particular port, use the `fuser` command. The `fuser` command provides the PID of the process using the port. For more information, see the man page of `fuser`.

Additions have been made to the `S98cms_ndd` script that enables the system to avoid network Denial of Service (DoS) attacks. Specifically, the attempt is to avoid TCP SYN attacks by increasing the TCP queue for unestablished connections and the TCP queue for established connections. This does not deter a TCP SYN attack from a system that has more resources allocated than the larger queues can handle, but it avoids the known TCP SYN attacks.

```
ndd -set /dev/tcp tcp_conn_req_max_q0  2048
ndd -set /dev/tcp tcp_conn_req_max_q   1024
```

Changing the default password encryption algorithm on RHEL

Unlike Solaris, RHEL uses SHA512 as the default password encryption algorithm. This enables long passwords and removes the need to change the encryption algorithm to something else.

Modify permissions of CMS user home directories as created by CMS application

When a new user is created, the system creates a new home directory for the user in `/export/home/[userid]`. The directory is created with permissions of `755`, and should be more restrictive. CMS now creates the user's home directory and modifies the permissions to `750`. Additional files created by users may be changed to this setting by running the `userperms.sh` script.

Controlling who can connect to the CMS system

The CMS Security Script creates the files `/etc/hosts.allow` and `/etc/hosts.deny`. Use these files to control which IP addresses are permitted to connect to the Avaya CMS system.

Note:
The CMS security script will NOT write over existing `/etc/hosts.allow` and `/etc/hosts.deny` files. To get the updated files, copy the `hosts.allow` and `hosts.deny` files from the CMS DVD `security/sec_files` directory to `/etc` on the system.:

`cp /cdrom/cdrom0/security/sec_files/hosts.allow /etc/`

`cp /cdrom/cdrom0/security/sec_files/hosts.deny /etc/`

To use the `/etc/hosts.allow` and `/etc/hosts.deny` files:

1. Edit `/etc/hosts.allow`

   This file contains the following settings:

   - `ALL : localhost`
   - `sshd : ALL`
   - `ALL : ALL : DENY`

   Note:
   Network services `rsh`, `rexec`, and `rlogin` are disabled on Avaya CMS systems. The lines in this file do not affect a service if the daemon for that service is not running.

This disables telnet from all remote hosts but still allows telnet via port forwarding from Supervisor users.

Note:
Avaya CMS Supervisor supports telnet and SSH connections.

2. Edit `/etc/hosts.deny`

3. It currently has the following entry:

   ```
   ALL : ALL
   ```

4. In order to allow certain IP addresses and subnets to connect to Avaya CMS system using a particular service, change file `/etc/hosts.allow` by replacing `ALL` with the permitted IP addresses.

The following table contains some examples of security setting use:

Example setting	Explanation of use
`in.telnetd : 10.8.10.0/255.255.255.0`	This setting allows telnet connections from all IP addresses from 10.8.10.1 to 10.8.10.255.
`sshd : 10.0.0.0/255.0.0.0`	This setting allows ssh connections from all IP addresses from 10.0.0.1 to 10.255.255.255.
`in.rshd :  10.8.31.100 10.8.31.55`	This setting allows connections from IP addresses 10.8.31.100 and 10.8.31.55.

Modifying crypto ciphers for the web client

To enable stronger ciphers with CMS Web, change the configuration of Tomcat configuration file to indicate what encryption standards to use.

Use the following procedure to modify crypto ciphers for the web client on the CMS server:

1. Change to the directory `/opt/cmsweb/tomcat/conf`.

   `cd /opt/cmsweb/tomcat/conf`

2. Copy `server.xml` to `server.xml.orig`.

   `cp server.xml server.xml.orig`

3. Locate the following section in `server.xml`:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="3500" scheme="https" secure="true"
               keystoreFile="/opt/cmsweb/cert/cmsweb.jks"
               keystorePass="cmsweb"
ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WIT
H_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE
_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA2
56,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_256_G
CM_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_
256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA
_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256"
               useServerCipherSuitesOrder="true"
               clientAuth="false"
sslEnabledProtocols="TLSv1.2,TLSv1.3" />
```

4. Modify the section to the following:

```
<Connector port = "8443" protocol = "HTTP/1.1" SSLEnabled = "true"
maxThreads = "3500" scheme = "https" secure = "true"
keystoreFile = "/opt/cmsweb/cert/cmsweb.jks"
keystorePass = "cmsweb"
clientAuth = "false"
sslEnabledProtocols = "TLSv1, TLSv1.1, TLSv1.2"
useServerCipherSuitesOrder = "true"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_
AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA
_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS
_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CB
C_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256
_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_
GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_CB
C_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_
SHA,TLS_RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA" />
```

Note:

Other Ciphers can be added or removed from this list based on customer preference. Any changes to the file constitutes permissive use.

Restricting access to the database

Use dbaccess to limit which CMS logins have ODBC/JDBC access to the CMS database. The CMS database has “open access” permissions as a standard feature which allows permission to any CMS login, connecting to the CMS server via ODBC/JDBC, to view any CMS table. No action is required if all CMS logins are allowed open access to the CMS database.

The dbaccess utility does not provide the ability to control which tables the CMS login has access to, or which ACD data the CMS login can view. The process of setting the secure database access is performed in two parts. First, all CMS login ids that are allowed CMS database access must be members of the UNIX group dbaccess. Second, you must execute the dbaccess option under the cmsadm menu.

Note:
Adding a single CMS login to the dbaccess group disables “open access” permissions for all users that are not members of the dbaccess group.

1. Each CMS login allowed ODBC/JDBC access to the CMS database must be added to the UNIX group dbaccess. To add CMS logins to the dbaccess group, enter:

   usermod -G dbaccess *cmslogin*

   Where *cmslogin* is the user id of the specific CMS login to be placed in the group. You must execute the usermod command for each CMS login that you wish to provide CMS database access.

2. To determine which logins are in the dbaccess group, enter:

   cat /etc/group | grep dbaccess

3. Open the **Avaya Call Management System Administration** menu. Enter:

   cmsadm

   The system displays the **Avaya Call Management System Administration** menu.

4. Select the dbaccess option. The system displays the following message:

```
Begin CMS DB Access Permissions changes
grant resource to "public";

Your CMS database currently has public access permissions to all resources. Do you
wish to revoke this access and only grant access to specific CMS users? [y,n,?]
```

5. Enter: **y**

   The process continues. The system displays the following messages:

```
Please wait while CMS Informix Database permissions are changed.
revoke resource from public;
revoke connect from public;
grant connect to cms;
grant connect to cmssvc;
Revoke resource from public on CMS database.
Please wait while connect permissions are granted for requested users
grant connect to <cmslogin>;
grant connect to <cmslogin>;
.
.
.
Changes to CMS DB Access Permissions finished.
```

Note:
The output will always display one “grant connect” message per CMS logid, including logids already in the `dbaccess` group with connect permissions.

After the changes are complete, you may use the CMS logids to run ODBC/JDBC clients and access the CMS database.

To remove ODBC/JDBC access permissions for CMS logids, first remove them from the UNIX `dbaccess` group then run `dbaccess` from the **Avaya Call Management System Administration** menu.

6. Remove ODBC/JDBC access permissions for CMS logids from the UNIX `dbaccess` group. Enter:

   `usermod -G "" `*`cmslogin`*

7. Open the **Avaya Call Management System Administration** menu. Enter:

   `cmsadm`

   The system displays the **Avaya Call Management System Administration** menu.

8. Select the `dbaccess` option. The system displays the following message:

```
Begin CMS DB Access Permissions changes
Please wait while connect permissions are granted for requested users
grant connect to  <cmslogin>;
.
.
.
Changes to CMS DB Access Permissions finished.
```

The UNIX `dbaccess` group information is re-set to only provide access permissions for members remaining in the UNIX `dbaccess` group.

Perform the Steps 9 through 11 to remove all the CMS logins from the UNIX `dbaccess` group and restore “open access” permissions to all the CMS logins.

9. Run the usermod command for each CMS login in the `dbaccess` group. Enter:

   usermod -G "" *cmslogin1*

   usermod -G "" *cmslogin2*

   usermod -G "" *cmslogin3*

10. Open the **Avaya Call Management System Administration** Menu. Enter:

    cmsadm

    The system displays the **Avaya Call Management System Administration** menu.

11. Select the `dbaccess` option. The system displays the following message:

```
Begin CMS DB Access Permissions changes

No CMS user ids are in UNIX group dbaccess.
If you proceed, the CMS database will
be set to public permissions access for all resources.
Do you really want to do this? [y,n,?]
```

12. Enter: **y**

    The process restores public permissions to the CMS database. The system displays the following messages:

```
Please wait while CMS Informix Database permissions are set to public.
grant resource to public;
revoke connect from cms;
revoke connect from cmssvc;
Grant resource to public on CMS database.
Changes to CMS DB Access Permissions finished.
```

Appendix A: CMS permissive use

CMS permissive use support policy

As of October 3, 2006, the following "Permissive Use" policy applies to CMS and should be taken into consideration when modifying the CMS system:

Call Management System (CMS) Standard Operating Environment

Under the terms of relevant hardware and software support contracts, Avaya will support the entire system, hardware and software, from end to end, managing the escalation and resolution of problems with any system component to the correct support organization. This includes hardware and software categorized as "standard" product. "Standard" product refers to configurations that have been initially designed, tested and certified by Avaya.

Some customers require the platform to perform other functions (for example: co-resident applications), or to connect with non-standard hardware configurations. Such configurations are specifically not recommended, but in the case where they are utilized, Avaya Global Services will continue to support the CMS application in a "permissive use" mode. For these non-standard configurations, the Avaya Global Services ITAC or Center

of Excellence will troubleshoot problems with the CMS application, but cannot and will not accept responsibility for end-to-end system integrity. When operating outside of a "standard" configuration, the customer has the added responsibility of managing the non-standard configuration and may incur additional charges when Avaya Global Services resources are required.

See Permissive Use statement below for a complete description of the permissive support policy and terms and conditions with respect to non-standard CMS configurations.

Permissive Use of Non-Standard CMS Configurations

Policy:

Avaya will allow and thereby support permissive use of non-standard networking, non-standard terminal equipment, and other application packages in conjunction with CMS. Avaya will not withdraw support of the CMS application if it is determined that other packages, applications, or hardware are running concurrently. The software packages and hardware connectivity that are running concurrently with the CMS may well be packages that are sold and supported by other Avaya organizations (for instance, Remote File Sharing Utilities, Token Ring LAN, or other physical interfaces including wallboards), as well as other vendor applications. Non-standard configurations are not be installed by Avaya personnel.

Avaya reserves the right to implement enhancements or modifications of this policy at any time without providing prior written or verbal notice to Avaya maintenance contract customers.

Responsibilities under the Policy:

Avaya:

Avaya's responsibilities are limited to correcting faults with the standard CMS application. CMS customers operating in a non-standard environment who are seeking assistance from Avaya will be subject to standard maintenance response times. They are not eligible for priority queuing. When a trouble is reported to Avaya, and it is determined that other applications or non-standard terminals, link or hardware connectivity are being used, Avaya may require that this non-standard hardware and software be removed from the

system and the system be returned to a standard configuration in order to be able to diagnose the CMS trouble. Reasonable and timely effort will be made to troubleshoot the issue prior to requiring the CMS to be returned to a standard configuration; however, this may be the only way to separate CMS troubles from other non-standard issues. This reconfiguration decision is the sole responsibility of the Avaya Tier III engineer.

Upgrades: If it is determined that standard Avaya upgrade processes will be impacted by the existence of non-standard configurations, Avaya will not perform said upgrade until the CMS is returned to an Avaya "standard" configuration.

Customer:

If required by Avaya, it will be the responsibility of the customer to perform a reconfiguration of the CMS to return it to a standard configuration. Customers must take notice that the CMS system may remain in a trouble state until this reconfiguration can be performed. Avaya will not be held responsible for any associated damages that may result from this period of delay.

Billing:

If troubleshooting can only be performed outside of the times of any applicable CMS software support contract (warranty or maintenance), the customer will be billed then-current premium Time and Material charges.

If it is determined that the trouble is no longer present after this re-configuration, the customer will be billed Time and Material charges for the trouble shooting effort, regardless of any pre-existing hardware or software contract agreements.

Note:

This policy is subject to change in the future and is reproduced here for reference purposes only.

Links to Avaya security resource

List of current versions of the security documents are shown below. Note that these documents typically change for each release. You can access these documents at www.avaya.com/support.

- Avaya CMS R18 documentation
- Avaya CMS R18 Software Installation, Maintenance and Troubleshooting for Linux®
- Avaya Call Management System Switch Connections, Administration & Troubleshooting
- Avaya Call Management System LAN Backup
- Avaya Call Management System Overview and Specification
- Avaya Call Management System Administration
- Avaya Call Management System External Call History Interface

Appendix B: CMS security/Hardening offer

CMS security / Hardening offer

The Avaya Enterprise Security Practice offers CMS Security Hardening, an in-depth review of the CMS system that identifies vulnerabilities. It configures the hardening measures needed to bring older CMS systems into compliance with today's security requirements. For new CMS systems, this custom configuration can also deliver a method to prevent multiple sessions from a single agent and to close inactive agent sessions automatically after a timeout period.

The following security measures can be included in a hardening engagement. Note that items with an asterisk have already been delivered by default in newer CMS systems and generally apply to CMS systems prior to R12 ONLY:

- Install any critical RHEL security patches not yet installed.
- Disable all unnecessary network daemons (services) for older CMS systems*.
- Reconfigure the RHEL system stack to reduce the risk of buffer overflow attacks*.
- Modify Telnet and FTP login banners to obfuscate operating system information.
- Disable direct login access to "root" ID*.
- Disable privileged accounts from accessing the system using FTP*.
- Modify network device driver characteristics to prevent IP forwarding and redirects*.
- Reconfigure TCP stack to use smarter TCP sequence numbers*.
- Tighten file permissions in /etc and its subdirectories*.
- Modify file permissions and ownership of user shells*.
- Unless CMS utilizes HA Auto-Sync package, remove any "`rhosts`" files in CMS users' home directories.
- Prevent users from sharing authentication credentials.
- Implement Password Aging: All CMS user accounts are required to change their password once every 186 days. Users are notified one week before password expires.
- Display a customized warning message for restricted use, prior to login prompt.
- Display of customized warning message, after authentication, of corporate security policies must be adhered to and that unauthorized usage may result in disciplinary action.
- Install a script to disable user accounts that have not been utilized for the past 90 days.
- Lock "anonymous" and FTP user accounts*.

- Schedule automatic nightly logoff of users.
- Install various logging packages for advanced auditing.