Avaya Call Management System Security

Release 21.0.2
Issue 2
June 2025

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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 Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, 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. Unless otherwise stated, 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

The following applies only 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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 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

(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 to comply 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, please contact your Avaya Sales Representative.

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 LLC.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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

This document describes optional security functionality available with Avaya Call Management System (CMS) running on the Red Hat Enterprise Linux (RHEL) operating system.

This document is intended for support personnel and customers who want more information about CMS security. To use this document, you must be familiar with CMS and the RHEL operating system.

Change history

The following table outlines the key changes in this document:

Issue	Date	Summary of changes
2	June 2025	Added details for using Avaya Identity and Access Management (IAM) in Configuring login settings for Avaya IAM on page 15.
1	June 2024	• Minor edits in the Introduction chapter. • Updated Local login authentication on page 10 to include information about enabling CMS to ignore the case of an Active Directory username. • Updated the steps in Configuring the choice of authentication service on page 13. • Updated the information in Disk encryption on page 23. • Added CMSADM backup encryption on page 23. • Updated Informix information in Database access on page 33. • Minor layout changes and edits.

Chapter 2: User login authentication

This section explains the login authentication methods that you can configure for CMS.

Related links

CMS user login options

You can configure the following methods of login authentication for CMS users:

- **Local login**

  Users can log in to CMS locally using the user ID and password administered locally in CMS.

- **LDAP login using Microsoft Active Directory**

  You can administer individual users for password authentication using Microsoft Active Directory (AD) to enable LDAP password authentication.

- **Enterprise login**

  The CMS Web Client can use an enterprise authentication service such as Microsoft Azure to authenticate user logins. The user still requires a login ID configured on CMS.

- **Certificate login**

  This method uses personal certificates for authentication. Joint Interoperability Test Command (JITC) certification requires this method of authentication.

Note:

- The user must have a CMS user ID for local, LDAP, and/or enterprise login methods.

- If you want to restrict a user to enterprise login only (web client only), do not assign a valid Linux password when you create the new user and do not set up LDAP authentication for the user. The absence of a Linux password and LDAP authentication blocks the user from logging in using a local login.

Related links

User login authentication on page 7

CMS user IDs

The user must have a CMS user ID for local, LDAP, and/or enterprise login methods. This applies even if the login method used does not prompt the user for their user ID, for example as with an enterprise login.

- **For non-LDAP local logins:**
  - The CMS user ID can have up to 31 alphanumeric characters and no special characters.
- **For LDAP local logins:**
  - The CMS user ID must match the user ID in Active Directory.
  - The CMS user ID can have up to 20 alphanumeric characters and no special characters.
- If you want to restrict a user to the enterprise login method (web client only), do not assign a valid Linux password when you create the new user and do not set up LDAP authentication for the user. The absence of a Linux password and LDAP authentication blocks the user from logging in using a local login.

Related links

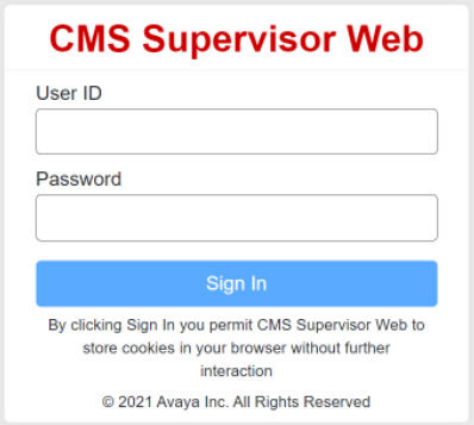
User login authentication on page 7

Web client user login window

CMS users see different login windows based on whether they have logged in using the local or enterprise login method.

Example: Local and LDAP login

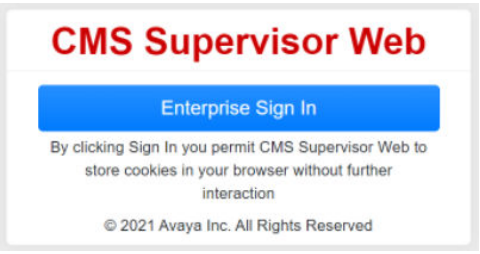
To log in to the Web Client, the user enters the CMS user ID and password and clicks **Sign In**.



Example: Enterprise login

To log in to the Web Client, the user clicks **Enterprise Sign In**.

- The enterprise authentication service manages the login authentication. The user must provide the login credentials based on how you configured enterprise login service, including any Multi-Factor Authentication (MFA).



Related links

User login authentication on page 7

Session timeouts and multiple login sessions prevention

By default, no timeouts exist for user or administrator login sessions on CMS. However, you can configure a **cron** job for this purpose. You can consult with Avaya Professional Services for help.

The primary use of CMS Supervisor is to run reports that automatically refresh. Therefore, CMS assumes that while a user is running a report that user is active.

Web client login limit

Beginning with CMS Release 19.2, CMS limits CMS Supervisor Web Client users to one active logon session. Each active login session consumes a CMS Supervisor user license.

- CMS stores the active sessions limit in the `/opt/cmsweb/data/system.properties` file.
- The previous checks for number of sessions from the same user or IP address remain. CMS applies those before checking the count in the `/opt/cmsweb/data/system.properties` file.

Minimized web client timeout

If a user minimizes their web client for too long, CMS will log out the user. CMS uses the *sessionTimeoutMinutes* value in the `/opt/cmsweb/data/system.properties` file for the timeout. The minimum/default setting is 4 minutes.

Related links

User login authentication on page 7

Local login authentication

CMS users are RHEL users. Therefore, for local login CMS uses the login and password authentication features of the RHEL operating system. Specifically, CMS uses the RHEL Pluggable Authentication Modules (PAM) to authenticate users.

- The CMS user ID can have up to 31 alphanumeric characters and no special characters.

Related links

User login authentication on page 7
Password complexity rules and considerations on page 10
Password expiration on page 12

Password complexity rules and considerations

The password complexity requirements for CMS are based on standard RHEL methodology using pluggable authentication modules (PAM).

⚠ Caution:

- This section will not train you on password authentication with PAM. You must refer to the RHEL documentation.
- If you do want to change the password complexity settings, Avaya recommends that you use the RHEL **`authconfig`** tool rather than directly making changes to the PAM files.
- Before making any changes to PAM, you must take a full CMS system backup. Use considerable caution when changes to PAM as any mistake can cause the system to deny logins.
- The password complexity rules do not apply to CMS users using LDAP authentication.

The PAM system authentication file (`/etc/pam.d/system-auth`) specifies the password rules, as shown in the example file below:

```
#%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        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so
```

```
password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3
authtok_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     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

The file has four sections:

- The `auth` rules apply to authentication.
- The `account` rules check if the account is locked or expired.
- The `password` rules process the requirements for password changes and complexity.
- The `session` rules configure the user sessions.

The default Secure Hash Algorithm (SHA) is SHA512. SHA512 should be used to encrypt the password, and the system should maintain the `/etc/shadow` file. If any aging conditions are met, the module is considered *sufficient* and the system allows the login. If this rule fails, the rule moves to the next PAM module, `pam_deny.so`, which denies the login.

Password complexity

The `pam_pwquality.so` module enforces password complexity. By default, it rejects new passwords that match any of the following criteria:

- Exceeds the number of consecutive characters set by the `maxrepeat` parameter.
- Contains the username in some form.
- Does not contain an upper case character.
- Does not contain a numeric character.
- Is part of a dictionary word in the `/usr/share/dict/words` dictionary.
- Is a palindrome.
- Is just a change in the upper and lower case of the old password.
- Is similar to the old password.
- Is a rotated version of the old password.
- Has not changed at least 10, or half the length of the new password if larger, of the existing characters. By default, for this calculation RHEL ignores characters after the 23rd character.

PAM password authentication provides strong security. However, it can make it difficult and frustrating for users to change their passwords. 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. Therefore, the longer and more complex the existing password, the more difficult it is to change the password to meet the complexity criteria.

You can modify the password complexity rules to work around this complexity. However, any relaxing of the default password complexity rules reduces the security of password authentication. Therefore, you must carefully consider any modification to password complexity.

Related links

Local login authentication on page 10

Password expiration

By default, CMS does not use password aging (forced password expiration). If required, you can activate password aging from 1 to 52 weeks.

- If enabled, password aging affects the passwords of all CMS and RHEL users except non-CMS user IDs such as *root*, *root2*, and *informix*.
- RHEL password aging does not affect LDAP authentication. The Microsoft AD service controls aging of LDAP user passwords.
- For details of configuring password aging, see the *Maintaining and Troubleshooting Avaya Call Management System* manual.

Related links

Local login authentication on page 10

LDAP login authentication

A CMS system using local authentication can also use LDAP authentication with Microsoft Active Directory (AD).

- To use Active Directory, you must install the LDAP package on CMS and administer CMS to connect to the AD server. See the following documentation:
  - The "*Administering LDAP*" section in the *Administering Avaya Call Management System* manual.
  - The "*Updating the LDAP authentication package configuration*" section in *Maintaining and Troubleshooting Avaya Call Management System* manual.
- The CMS user ID must match the user ID in Active Directory.
- The CMS user ID can have up to 20 alphanumeric characters and no special characters.
- The RHEL password complexity settings do not apply to LDAP authentication.

Related links

User login authentication on page 7
Disabling LDAP username case sensitivity on page 12

Disabling LDAP username case sensitivity

About this task

The CMS and Active Directory user IDs must match. However, if required you can configure CMS to ignore the case of Active Directory usernames.

Procedure

1. Add the line `ignorecase yes` to the `/etc/nslcd.conf` file.
2. Run `service nslcd restart` to restart the service.

Related links

LDAP login authentication on page 12

Enterprise login authentication

For access to the CMS web client, you can configure CMS to use an enterprise authentication service such as Microsoft Azure, Okta, or Avaya Identity and Access Management (IAM).

Related links

User login authentication on page 7
Configuring the choice of authentication service on page 13
Configuring login settings for Avaya IAM on page 15
Configuring login settings for Microsoft Azure on page 16
Configuring login settings for Okta on page 17
Configuration Helper tool on page 19
Troubleshooting enterprise authentication on page 20

Configuring the choice of authentication service

About this task

Use this procedure to set the authentication methods CMS supports for CMS user and superuser access.

Before you begin

- If you intend to use an enterprise authentication service for CMS web client access, complete the registration of the CMS application with the enterprise authentication service. You will require information from that registration for CMS configuration.

Procedure

1. Log in to the CMS server as a root user.
2. Open the `/opt/cmsweb/data/login.properties` file in a text editor.
3. To set the authentication method CMS uses for the *cms* and *cmssvc* accounts, set the `login.superUserOption` value as follows:

`login.superUserOption=<authentication service>` where:

- *<authentication service>* is the choice of authentication service or services using the following values:
  - *Password* = Use local login for CMS. Also used for CMS web client login unless an enterprise authentication service is selected.
  - *Azure* = Use the Microsoft Azure enterprise authentication service for CMS web client login.
  - *Iam* = Use the Avaya Identity and Access Management service for CMS web client login.
  - *Okta* = Use the Okta enterprise service for CMS web client login.
- You can enter *Password* and/or one of *Azure*, *Iam*, or *Okta*.
- Separate multiple values with a comma. For example: `login.superUserOption=Password,Azure`

4. To set the authentication methods CMS uses for users other than *cms* and *cmssvc*, set the `login.regularUserOption` as follows:

   `login.regularUserOption=<authentication service>` where:

   - *<authentication service>* is the choice of authentication service or services using the following values:
     - *Password* = Use local login for CMS. Also used for CMS web client login unless an enterprise authentication service is selected.
     - *Azure* = Use the Microsoft Azure enterprise authentication service for CMS web client login.
     - *Iam* = Use the Avaya Identity and Access Management service for CMS web client login.
     - *Okta* = Use the Okta enterprise service for CMS web client login.
   - You can enter *Password* and/or one of *Azure*, *Iam*, or *Okta*.
   - Separate multiple values with a comma. For example: `login.superUserOption=Password,Azure`
5. To have CMS use a proxy to connect to the server for token authentication:
   a. Set the `login.useProxy` variable to `yes`.
   b. Set the `login.proxy` variable to the URL of the proxy. For example: `login.proxy=http://proxy.glb.avayacloud.com:50443`
6. If you selected any of the enterprise authentication services, you also need to configure CMS variables for connection to that authentication service:
   - **Avaya IAM:** See Configuring login settings for Avaya IAM on page 15.
   - **Microsoft Azure:** See Configuring login settings for Microsoft Azure on page 16.

- **Okta:** See Configuring login settings for Okta on page 17.

7. Restart the web client process using the `cmsweb stop` and `cmsweb start` commands.
   - Restarting the web client process ends all active logins but does not require CMS downtime. CMS applies the `login.properties` file changes when users log in again.

Related links

Enterprise login authentication on page 13

Configuring login settings for Avaya IAM

About this task

If you have selected *Iam* as an authentication method (see Configuring the choice of authentication service on page 13), use this process to set the CMS variables for Avaya Identity and Access Management (IAM) connection.

Before you begin

Ensure that you have the following information from the process of registering the CMS application with Avaya IAM:

- The *Company Domain*.
- A *Client ID*.
- The *Redirect URI*.
- The *Front-channel Logout URL*.
- The FQDN of the CMS application and the port.

Procedure

1. Set the `login.iam.authority` value as follows:

   `login.iam.authority=https://<company>` where:

   - <*company*> is the company domain registered with the enterprise authentication service and may be prefixed by a sub-domain identifying the service.

2. Set the `login.iam.clientID` value as follows:

   `login.iam.clientId=<client ID>` where:

   - <*client ID*> is the value provided by the enterprise authentication service.

3. Set the `login.iam.userInfoUrl` value as follows:

   `login.iam.userInfoUrl=https://<company>/idp/userinfo.openid` where:

   - <*company*> is the company domain registered with the enterprise authentication service and may be prefixed by a sub-domain identifying the service.

4. Set the `login.iam.redirectUriSignin` value as follows:

`login.iam.redirectUriSignin=https://<cmshost>:<port>/CMSWeb/` where:

- <*cmshost*> is the fully-qualified domain name for the CMS application.
- <*port*> is the port administered for enterprise authentication service integration. The default is 8443.
- The value must match the *Redirect URI* configured for CMS in the authentication service.

5. Set the `login.iam.postLogoutRedirectUri` value as follows:

   `login.iam.postLogoutRedirectUri=https://<cmshost>:<port>/CMSWeb/` where:

   - <*cmshost*> is the fully-qualified domain name for the CMS application.
   - <*port*> is the port administered for enterprise authentication service integration. The default is 8443.
   - The value must match the *Front-channel Logout URL* configured for CMS in the authentication service.

6. Restart the web client process using the `cmsweb stop` and `cmsweb start` commands.
   - Restarting the web client process ends all active logins but does not require CMS downtime. CMS applies the `login.properties` file changes when users log in again.

Related links

Enterprise login authentication on page 13

Configuring login settings for Microsoft Azure

About this task

If you have selected *Azure* as an authentication method (see Configuring the choice of authentication service on page 13), use this process to set the CMS variables for Microsoft Azure connection.

Before you begin

Ensure that you have the following information from the process of registering the CMS application with Microsoft Azure:

- An *Application ID*.
- A *Tenant ID*.
- The *Redirect URI*.
- The *Front-channel Logout URL*.
- The FQDN of the CMS application and the port.

Procedure

1. Set the `login.aad.clientId` value as follows:

`login.aad.clientId=<application ID>` where:

- *<application ID>* is the value provided by the enterprise authentication service.

2. Set the `login.aad.authority` value as follows:

   `login.aad.authority=https://login.microsoft.com/<tenant ID>` where:

   - *<tenant ID>* is the value provided by the enterprise authentication service.

3. Set the `login.aad.msGraphEndpointHost` as follows:

   `login.aad.msGraphEndpointHost=https://graph.microsoft.com/.`

4. Set the `login.aad.redirectUriSignin` value as follows:

   `login.aad.redirectUriSignin=https://<cmshost>:<port>/CMSWeb/` where:

   - *<cmshost>* is the fully-qualified domain name for the CMS application.
   - *<port>* is the port administered for enterprise authentication service integration. The default is 8443.
   - The value must match the *Redirect URI* configured for CMS in the authentication service.

5. Set the `login.aad.postLogoutRedirectUri` value as follows:

   `login.aad.postLogoutRedirectUri=https://<cmshost>:<port>/CMSWeb/` where:

   - *<cmshost>* is the fully-qualified domain name for the CMS application.
   - *<port>* is the port administered for enterprise authentication service integration. The default is 8443.
   - The value must match the *Front-channel Logout URL* configured for CMS in the authentication service.

6. Restart the web client process using the `cmsweb stop` and `cmsweb start` commands.

   - Restarting the web client process ends all active logins but does not require CMS downtime. CMS applies the `login.properties` file changes when users log in again.

Related links

Enterprise login authentication on page 13

Configuring login settings for Okta

About this task

If *Okta* is one of the selected authentication methods (see Configuring the choice of authentication service on page 13), you must set the variables for Okta connection.

Before you begin

Ensure that you have the following information from the process of registering the CMS application with Microsoft Azure:

- The *Company Domain*.
- A *Client ID*.
- The *Redirect URI*.
- The *Front-channel Logout URL*.
- The FQDN of the CMS application and the port.

Procedure

1. Set the `login.okta.domain` value as follows:

   `login.okta.domain=https://<company>.oktapreview.com` where:

   - <*company*> is the company domain registered with the enterprise authentication service.

2. Set the `login.okta.clientId` value as follows:

   `login.okta.clientId=<client ID>` where:

   - <*client ID*> is the value provided by the enterprise authentication service.

3. Set the `login.okta.userInfoUrl` value as follows:

   `login.okta.userInfoUrl=https://<company>.oktapreview.com` where:

   - <*company*> is the company domain registered with the enterprise authentication service.

4. Set the `login.okta.redirectUriSignin` value as follows:

   `login.okta.redirectUriSignin=https://<cmshost>:<port>/CMSWeb/` where:

   - <*cmshost*> is the fully-qualified domain name for the CMS application.
   - <*port*> is the port administered for enterprise authentication service integration. The default is 8443.
   - The value must match the *Redirect URI* configured for CMS in the authentication service.

5. Set the `login.okta.postLogoutRedirectUri` value as follows:

   `login.okta.postLogoutRedirectUri=https://<cmshost>:<port>/CMSWeb/` where:

   - <*cmshost*> is the fully-qualified domain name for the CMS application.
   - <*port*> is the port administered for enterprise authentication service integration. The default is 8443.
   - The value must match the *Front-channel Logout URL* configured for CMS in the authentication service.

6. Restart the web client process using the `cmsweb stop` and `cmsweb start` commands.
   - Restarting the web client process ends all active logins but does not require CMS downtime. CMS applies the `login.properties` file changes when users log in again.

Related links

Enterprise login authentication on page 13

Configuration Helper tool

Instead of editing the `/opt/cmsweb/data/login.properties` file, you can use the `/opt/cmsweb/bin/configlogin.sh` script to configure the CMS user login properties.

The following example shows how you can use the program:

```
$ ./configlogin.sh
Login option(s) for super users:
1) Use Linux password? (y/n) default : y
2) Use Azure? (y/n) default : n
3) Use Okta? (y/n) default : y
4) Use Iam? (y/n) default: n
Login option(s) for regular users:
1) Use Linux password? (y/n) default :
2) Use Azure? (y/n) default : n
3) Use Okta? (y/n) default : y
4) Use Iam? (y/n) default: n
Enter Okta domain: https://xyzcompany.okta.com
Enter Okta Client ID: 0oa9e38araOYA1Nfm5d7
Enter token verificaiton URL: (default https://xyzcompany.okta.com/oauth2/default/v1/
userinfo)
Enter host:port for CMS Web URL : (default cmsavm53.(none):8443)
Use a proxy for access token verification? (y/n) default :
```

New configuration:

```
login.superUserOption=Password,Okta
login.regularUserOption=Password,Okta
login.aad.clientId=ApplicationID
login.aad.authority=https://login.microsoftonline.com/TenantID
login.aad.msGraphEndpointHost=https://graph.microsoft.com
login.aad.redirectUriSignin=https://Host:8443/CMSWeb/
login.aad.postLogoutRedirectUri=https://Host:8443/CMSWeb/
login.okta.domain=https://xyzcompany.okta.com
login.okta.clientId=0oa9e38araOYA1Nfm5d7
login.okta.userInfoUrl=https://xyzcompany.okta.com/oauth2/default/v1/userinfo
login.okta.redirectUriSignin=https://cmsavm53.(none):8443/CMSWeb/
login.okta.postLogoutRedirectUri=https://cmsavm53.(none):8443/CMSWeb/
login.useProxy=no
login.proxy=Proxy
login.requireCertificate=no
Save the new configuration? (y/n) y
```

Related links

Enterprise login authentication on page 13

Troubleshooting enterprise authentication

Use the following troubleshooting tips if CMS users can view the Enterprise Login page but cannot log in successfully:

- Verify if CMS can connect to the network using the DNS. The login cannot succeed if the DNS does not recognize CMS or if CMS and the enterprise login method cannot identify each other on the network.
- Verify that you created the user in CMS and in the enterprise authentication service.
- Verify that the username is the same in CMS and in the enterprise authentication service.

Related links

Enterprise login authentication on page 13

Certificate login authentication

Certificate login authentication prevents users from logging in to CMS without having a matching personal certificate.

If enabled, when a user tries to log in, CMS sends a list of trusted certificate authorities to the user's browser. The browser selects, or prompts the user to select, a personal certificate to send back to CMS. CMS verifies the common name (CN) in that personal certificate against the user ID and username in CMS.

- For CMS, you can use personal certificates stored in a Common Access Card (CAC) or a certificate store such as Microsoft Cert Store.
- Using personal certificates is a requirement of JITC (The Joint Interoperability Test Command) certification. Federal and DoD (Department of Defense) employees must use personal certificates encoded and provided using a CAC.

Related links

User login authentication on page 7
Configuring certificate login authentication on page 20

Configuring certificate login authentication

About this task

You can configure CMS certificate login authentication using the `/opt/cmsweb/data/login.properties` configuration file. This procedure illustrates setting the variables and options in the `login.properties` file to configure certificate login.

Before you begin

- Import the certificate authority root certificate into the CMS web key store (`/opt/cmsweb/cert/cmsweb.jks`). For example:

```
keytool -import -trustcacerts -alias -file -keystore /opt/cmsweb/cert/cmsweb.jks
```

Procedure

1. Log in to the CMS server as a *root* user.
2. Open the `/opt/cmsweb/data/login.properties` configuration file.
3. Set `login.requireCertificate` to `login.requireCertificate=Yes`
4. Restart the web client process using the `cmsweb stop` and `cmsweb start` commands.
   - Restarting the web client process ends all active logins but does not require CMS downtime. CMS applies the `login.properties` file changes when users log in again.

Related links

Certificate login authentication on page 20

Chapter 3: Encryption

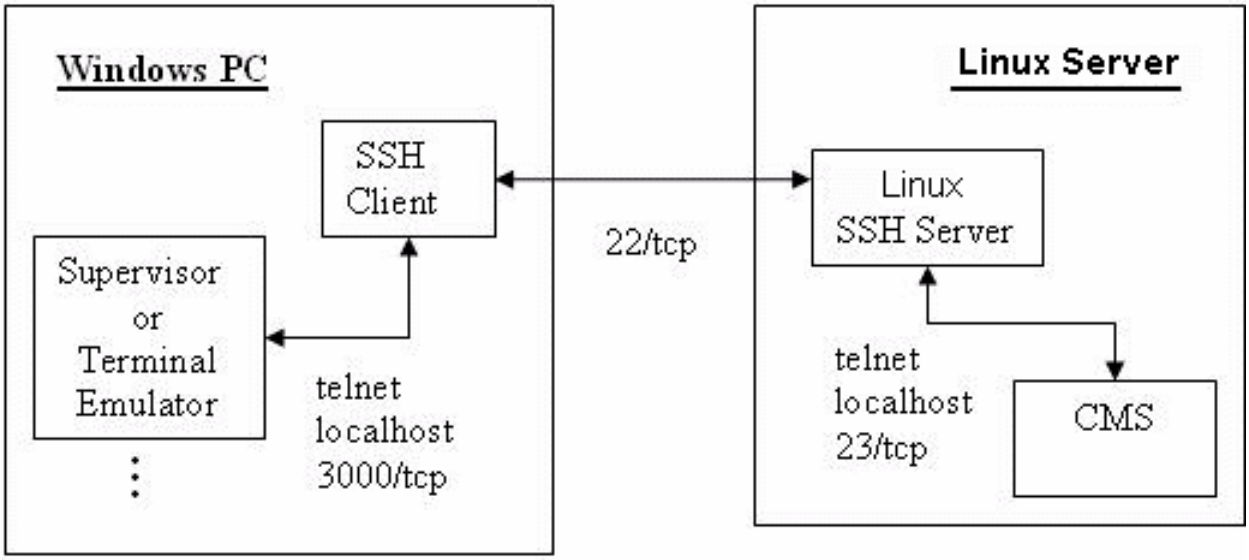
This chapter describes the following encryption information in CMS:

- Encryption when using SSH and telnet
- Disk encryption

Using SSH and telnet

When logging on using the CMS Supervisor PC Client, Secure Shell (SSH) is the default connection. On the PC Client, an SSH client package creates the SSH tunnel and encrypts and decrypts the SSH connection. Also, the Microsoft Crypto API provides password encryption and decryption functionalities. The login and password information stored in the registry is encrypted.

The following figure illustrates the connectivity between the various components:



The PC Client uses an SSH wrapper around the underlying telnet. Thus, telnet cannot be disabled on the CMS server when using the PC Client.

To improve telnet security on the CMS server, the telnet service can be locked down to only be used by the local host by editing the following files:

- `/etc/hosts.allow`

  Add the following lines:

  ```
  # allow telnet only from within the server
  in.telnetd : localhost
  ```

- `/etc/hosts.deny`

  Add the following lines:

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

Other points to consider:

- 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 at run time. A variety of industry-standard algorithms, such as 128/256-bit AES, 3des, chacha20, 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 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 following file for the current `ENCRYPT_METHOD` value:

  `/etc/login.defs`
- Beginning with CMS Release 19.2, direct root SSH connections are not allowed. This update is for security purposes.
- Supported Key Exchange (kex) algorithms have been reduced for security purposes.

Disk encryption

By default, CMS no longer encrypts disks and partitions with CMS data using LUKS encryption. This encryption is generally redundant because supported cloud providers encrypt by default and VMware supports disk encryption natively.

CMSADM backup encryption

CMSADM backups can be encrypted. The system identity variables stored in the backup are secured to ensure they are not disclosed or modified during the backup, storage, or

restore process. For more information about backup encryption options, see *Maintaining and Troubleshooting Avaya Call Management System*.

FIPS 140-2

CMS provides the option to turn on the Federal Information Processing Standard (FIPS) 140-2 compliant mode which implements stronger encryption for the following interfaces:

- SSH communications used by the CMS Supervisor PC Client
- HTTPS communications used by the CMS Supervisor Web Client

When FIPS 140-2 mode is enabled, CMS will only provide the FIPS-approved modules for SSH and HTTPS connections.

CMS does not adopt FIPS 140-2 encryption for ODBC or JDBC connections since these are considered optional. However, beginning with CMS Release 19.0, the ODBC or JDBC connection can be optionally encrypted.

Beginning with CMS Release 19.1, the connection between CMS and Communication Manager Release 8.1.2 or later is encrypted.

To activate FIPS 140-2, use the **`cmssvc`** command, choosing the **`security`** option to enable or disable the FIPS 140-2 mode. For more information about FIPS 140-2 mode, see *Maintaining and Troubleshooting Avaya Call Management System*.

Chapter 4: General security options

This chapter describes general security options that you might want to implement on your CMS deployment:

- Operating system (OS) security
- Authentication and encryption
- Application security

Operating system security

Avaya provides support for disabling standard services only after you follow the standard procedures documented in *Administering Avaya Call Management System* and *Maintaining and Troubleshooting Avaya Call Management System*. One of these standard procedures is running the CMS Security script **`cms_sec`**. This script installs core security updates and hardening.

These procedures can be used by customers, business partners, or Avaya Professional Services associates.

This section also describes any operating system software you must not use as part of a CMS deployment.

For other operating system hardening not discussed in this document, consult Avaya Professional Services to determine if other CMS modifications are available.

Virus scanning software

Avaya allows customers install AV/malware software themselves based on certain guidelines/ criteria. The only anti-virus products that have been tested with CMS are:

- Microsoft Defender
- McAfee / Trellix

Limitations

- 15% of system resources must be reserved for on-access scanning during normal/peak times and the standard CMS capacity scaled back accordingly. If on-access scanning is seen to consume more than 15% of resources then CMS capicity must be scaled back to account for this.

- On-demand scans only during off-peak times
  - On-demand scans can consume upto 35% of system resources
- No scanning of backup locations
- Exclude the following directories from the on-access scans
  - /cms/pbx – the location for spi.log/spi.err
  - /cms/cmstables – the location for external call records

Customer Responsibilites

- Customers may deploy 3rd party Anti-Virus/Malware software alongside the Avaya product.
- Customer deploys 3rd party applications at their own risk.
- Customer is responsible for testing prior to deployment.
- Customer is responsible for ensuring there are no TCP/UDP port conflicts and other protocol conflicts.
- Customer is responsible for ensuring adequate hardware is available to meet the requirements of both the Avaya applications and 3rd party applications.
- Customer is responsible for monitoring performance of the OS and applications, including these symptoms of performance degradation:
  - Missed or excessive alarms
  - Dropped remote access sessions
  - Slow user interface response
- During the course of an Avaya support engagement, the customer may be required to uninstall the 3rd party software if it is suspected to be a key contributor to, or the root cause of an issue.
- For those failure conditions directly or indirectly related to a 3rd party product, Avaya may, at its sole discretion, remove the 3rd party product or require the customer to remove the third-party product before proceeding with diagnostics and troubleshooting.
- Customer may need to remove 3rd party software before upgrading the product.

RHEL log file management

For logging related to RHEL operations, CMS uses the standard deployment and default settings of the RHEL **`logrotate`** tool. For logging specific to the CMS application, relevant log files are documented in the following documents:

- *Deploying Avaya Call Management System*
- *Maintaining and Troubleshooting Avaya Call Management System*
- *Administering Avaya Call Management System*

This section summarizes using **`logrotate`** for CMS. You can decide whether to change the **`logrotate`** settings. For more information about **`logrotate`**, see RHEL documentation.

The **logrotate** tool is a standard RHEL log file manager. The **logrotate** tool is used to cycle log files by removing or archiving old files and creating new log files. In summary, **logrotate** rotates log files so that older copies of the log files can be kept for a longer duration.

The **logrotate** rules of operation are found in the `/etc/logrotate.conf` configuration file. The following is an excerpt from the `/etc/logrotate.conf` configuration file deployed by default on CMS:

```
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
```

All the lines in the configuration file define global options that apply to every RHEL log file. In the above excerpt, log files are rotated weekly, and rotated log files are kept for four weeks.

You can modify the `/etc/logrotate.conf` configuration file and 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 where you can define the configuration options.

RHEL system auditing

For RHEL auditing operations, CMS uses the standard deployment and default settings of the RHEL Audit tool. You can modify these settings if desired.

This section summarizes how you use the auditing tools for CMS. You can decide whether to change the auditing tool settings. For more information about the auditing tools, see RHEL documentation. The RHEL documentation provides helpful examples for optional uses of the auditing tools.

CMS uses the standard RHEL auditing tools with standard default settings. CMS stores audit events in the `/var/log/audit/audit.log` file. The RHEL auditing system operates on a set of rules that define what to capture in the audit log files. The audit log rules are found in the standard directory at `/etc/audit/audit.rules`.

You can specify auditing rules on the command line with the **auditctl** utility. However, rule modifications made using the **auditctl** utility do not persist across reboots. That is, every time you reboot the CMS server, RHEL does not save your rule modifications. You can also write auditing rules in the `/etc/audit/audit.rules` file.

By default, CMS is set up with the following auditing rules:

```
# This file contains the auditctl rules that are loaded
# whenever the audit daemon is started

# First rule - delete all
-D

# Increase the buffers to maximum allowed in the
#  kernel
-b 8192

# Kernel failure conditions trigger printk
 -f 1
```

The following sections contain information on two aspects of RHEL auditing that you might find useful.

Defining file system rules

Using file system rules (also known as file watches) in the auditing tool, you can audit when a user accesses a particular file or a directory. The following is an example of how to define a file system rule using the **auditctl** command:

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

Where:

- *path_to_file* is the file or directory that is audited.
- *permissions* is the permissions that are logged, which consist of the following permissions:
  - 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.

Defining system call rules

Using system call rules in the auditing tool, you can audit system calls that a program makes. The following is an example of how to define a system call rule using the **auditctl** command:

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 **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 the following: **task**, **exit**, **user**, or **exclude**.
- *system_call* specifies the system call by its name.
- *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.

Persisting audit rule changes across reboots

For audit rules to persist across reboots, include the rules in the `/etc/audit/audit.rules` file. Changes to the rules must be entered using the same argument syntax used with the **auditctl** command.

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
```

```
# First rule - delete all
-D

# Increase the buffers to maximum allowed in the
#  kernel
-b 8192

# Kernel failure conditions trigger printk
 -f 1

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

Refer to the **auditd**, **auditctl**, and **audit.rules** man pages for detailed information about the available auditing and logging options.

Viewing and searching audit logs

You can use the **ausearch** command to search the audit logs without deciphering the formatting used in the `audit.log` file. Refer to the **ausearch** man page for a detailed description of the available options.

Custom banner messages

When users log on, CMS displays banner messages containing legal warnings or system information that is important to the users. You can customize these messages to obscure OS or application information, or to display a legal access warning, restricted warning for telnet users, or corporate policy for illegal computer activity.

By default, a banner message is not enabled on CMS. The banner message is not a click-through screen; it is a statement that CMS displays to the user.

Note:

The system displays banner messages only when a user logs in to an interactive terminal session. The system does not display banner messages for CMS Supervisor PC client users.

The following is an example of warning text in a banner:

```
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.
```

Web Client interface pre-login banner message

You can enable or modify the banner message displayed to a user before the login screen in the CMS Supervisor Web Client interface. To enable or modify the pre-login message, edit the following file to add the desired message:

`/opt/cmsweb/preloginbanner/banner.txt`

Web Client interface post-login banner message

You can enable or modify the banner message displayed when users log on to the CMS Supervisor Web Client interface. To enable or modify the post-login message, edit the following file:

`/opt/cmsweb/banner/banner.txt`

Editing and activating the Terminal interface banner message

You can modify the banner message displayed when logging on to the Terminal interface. To modify the message, edit the following file:

`/etc/issue.net`

To activate the banner for the Terminal interface, remove the `#` symbol from the following line in the `/etc/ssh/sshd_config` file:

```
#Banner
```

After editing and saving the `/etc/ssh/sshd_config` file, run the following command:

`systemctl restart sshd`

Email and SMTP

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

DNS and NFS

There is no support for sharing file systems to and from CMS servers.

If you modify or use the `hosts.allow` and `hosts.deny` files for access control, servers or files that control name resolution (Domain Name Servers or entries in the `/etc/hosts` file) must be under appropriate administrative control within the customer network. Doing this prevents an attacker from leveraging DNS services to enter a system.

By default, the `/etc/hosts.allow` file is configured to block all telnet connects except localhost.

By default, the `/etc/hosts.deny` file is configured to block all network connections not explicitly allowed in the `/etc/hosts.allow` file.

User file permissions and masks

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

You should not change the umask or file permissions on any CMS files as it can adversely impact CMS operations.

Chapter 5: CMS application security

Communication Manager ACD connections

CMS and Communication Manager connect using a data link that implements a proprietary binary protocol called the Switch Processor Interface (SPI). Access is controlled by IP address. Communication Manager sends ACD configuration information and ACD-related events to CMS using this proprietary protocol over the communication channel.

Beginning with CMS Release 19.1, the SPI data link is encrypted using TLS 1.3 when the CMS is connected to a Communication Manager Release 8.1.2.0 or newer system. Before these specific versions of CMS and Communication Manager, SPI link encryption was not available.

Application-level logging

There are several application logs within CMS. The most detailed application audit trails can be traced using the following log files:

- `/cms/install/logdir/admin.log`
- `/cms/pbx/acd<N>/spi.errlogs` (where <*N*> is the ACD number)
- `/cms/db/log/admin_chg.log`

The `admin.log` file records administrative changes to the CMS application.

The `spi.err` file logs show the information for setting up and debugging ACD links. These logs are intended for support, but can provide a partial audit trail for customers.

The `admin_chg` records all CMS administration changes from the client.

For more information about log files, see *Maintaining and Troubleshooting Avaya Call Management System*.

Database access

The HCL Informix database is embedded in the CMS application. CMS users do not log in to the Informix database or have any privileges within the Informix subsystem. All access to the Informix database is via the CMS application.

An optional ODBC or JDBC interface is available. Customers must activate and set up the ODBC or JDBC connection. The ODBC or JDBC connection can be configured for TLS or SSL encryption. This interface allows direct SQL queries of the Informix database but does not allow any CMS data changes.

Customers can use the ODBC or JDBC interface to create custom tables in the database available for use when creating CMS Supervisor Designer reports.

For more information about the ODBC or JDBC interface used with CMS, including details on how to restrict which logins have access to this interface and how to configure TLS or SSL encryption, see *Using ODBC and JDBC with Avaya Call Management System*.

Chapter 6: CMS network security

This chapter describes how the RHEL networking component helps to implement the various security features in CMS.

Firewall recommendations

Avaya recommends the CMS and CMS Supervisor clients to remain behind a firewall for protection from the Internet.

For more information about which ports are open or closed by default, see *Port Matrix for Avaya Call Management System*.

On RHEL, 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 security option of the **`cmssvc`** command. For more information about how to turn on or turn off the firewall, see *Maintaining and Troubleshooting Avaya Call Management System*.

Limiting external access to RHEL services

The CMS security script that runs during installation creates the following files:

- `/etc/hosts.allow`
- `/etc/hosts.deny`

Use these files to control which IP addresses are permitted to connect to the CMS server. Note that settings in `/etc/hosts.allow` cannot re-enable any services disabled through other means.

Note:

The entries in the `/etc/hosts.allow` and `/etc/hosts.deny` files are only honored when TCPWRAPPERS are enabled. TCPWRAPPERS are enabled by default.

For example, you might 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

Additional information about services configuration files are found in Controlling connections to CMS on page 40.

Limiting root access

Disabling root SSH logins

With CMS Release 19.2 and later, remote root access is denied by default. This section describes how customers can modify versions of CMS before Release 19.2 to deny remote root login. The method described in this section is how CMS Release 19.2 is deployed by default to deny remote root access.

To prevent root logins using the SSH protocol, edit the following SSH daemon configuration file:

`/etc/ssh/sshd_config`

Change the line that reads:

```
#PermitRootLogin yes
```

to

```
#PermitRootLogin no
```

This change 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.

With CMS Release 19.2.0.1 and later, the PermitRootLogin parameter has the new `without_password` default value that prevents direct root login without key authentication. This setting enables applications, such as the CMS High Availability Admin Sync, to access the root login using key authentication. If PermitRootLogin is set to `no`, the CMS High Availability Admin Sync cannot operate properly.

Network services

Network services can pose many risks for RHEL systems. Some of the primary issues are the following:

- Denial of Service attacks (DoS) – By flooding a service with requests, a DoS 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 use 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 that 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 access 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 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 Tools named:

- system-config-services
- ntsysv
- chkconfig

See the man pages of these commands for usage information.

Disabling RHEL services

Custom scripts or other custom integration added after the installation as part of an Avaya Professional Services offer might 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)
- Font Server (7100/tcp)
- FTP (inbound - 21/tcp)
- Kerberos V5 Warning Message Daemon (88/tcp, 88/udp)
- Name (42/udp)
- NFS Client (lockd - 4045/tcp, 4045/udp)
- NFS Server (2049/tcp, 2049/udp)
- NISClient
- Printer (Network printing services, local printing is enabled - 515/tcp)
- Rexec (512/tcp)
- Rlogin (513/tcp)
- Rsh (514/tcp)
- Sendmail (inbound - 25/tcp)
- Spray (100012/tcp, 100012/udp)
- Syslog (514/udp)
- Talk (517/tcp)
- Time Service (37/tcp, 37/udp)
- UUCP Network services (540/tcp)
- 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 is configured for clients, but it can be restricted to the local host so that it does not respond externally.

Review of port usage

CMS system can be placed behind a packet filtering firewall, although support for such configurations is not provided, especially when Network Address Translation (NAT) occurs. See the list below of port requirements for various aspects of CMS operations. Note that many CMS servers receive additional customization and configuration to add to this list or make some optional items mandatory.

The following ports administered for ACDs can be changed:

- 22/tcp ssh: optional, can be used by the CMS Supervisor PC Client or Web Client
- 23/tcp telnet: used by CMS Supervisor; optional for Terminal Emulator

Optional ports:

- 21/tcp: ftp, used by a Professional Services offer
- 25/smtp: sendmail, used by a Professional Services offer and SAL Gateway
- 37/tcp time: used by a Professional Services offer
- 111/tcp/udp rpcbind: used by CDE
- 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 (Professional Services offer). Also required for remote tape copy (provisioning)
- 515/tcp, udp: Printer server
- 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
- 5011/5012: ASAI
- 5160/tcp: SNMP
- 5107/tcp, 5108/tcp: SAL Gateway
- 5678: LAN Gateway
- 6001/tcp: X11
- 6060: Geotel
- 7443/tcp: SAL Gateway
- 8000/tcp: SAL Gateway

- 8089/tcp, Apache Tomcat: used by CMS Supervisor Web Client
- 8080/tcp, 8443/tcp: CMS Supervisor Web Client
- 9100/tcp, udp: hp-printers
- 9980: Link Admin
- 9999: CVLan
- 32771-32772/tcp and udp: Used by NFS status daemon (necessary if NFS backup is being used)
- 50000/tcp, 50001/tcp: Informix ODBC/JDBC

Note:

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

Additions are made to the **S98cms_ndd** upgrade 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 script does not deter a TCP SYN attack from a system with more resources allocated than the larger queues can handle, but it avoids the known TCP SYN attacks. The following shows the lines in the script:

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

Changing permissions of CMS user home directories created by CMS

When a new user is created, the system creates a new home directory for the user in the following location:

`/export/home/<userid>`

In older releases of CMS, the directory was created with permissions of 755 and those permissions 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 connections to CMS

The CMS security script creates the following files:

- `/etc/hosts.allow`
- `/etc/hosts.deny`

You can edit these files to control which IP addresses are allowed or denied access to a CMS server.

This document does not replace official RHEL documentation for editing and usage of the `/etc/hosts.allow` and `/etc/hosts.deny` files. CMS implements the standard use of these files within RHEL. For more information, see RHEL documentation.

The following table has some examples of entries that could be added to the `/etc/hosts.allow` file to restrict access to CMS. These examples are provided to give you an idea of what is possible.

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.

Changing crypto ciphers for the Web Client

About this task

To enable stronger ciphers when using the CMS Supervisor Web Client, you can change the configuration of Tomcat configuration file to indicate which encryption standards to use.

Important:

Other ciphers can be added or removed from the `server.xml` list based on your preference. Any changes to the file constitute permissive use.

Procedure

1. Log on to the CMS server as an administrator.
2. Move to the Tomcat configuration file directory using the following command:

   `cd /opt/cmsweb/tomcat/conf`
3. Make a backup copy of the `server.xml` file using the following command:

   `cp server.xml server.xml.orig`

4. Open the file for editing using the following command:

   vi server.xml

5. Locate the following information found in the file:

```
<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" />
```

6. You can change the configuration of Tomcat configuration file to indicate which encryption standards you want to use.
7. Save and close the file.

Restricting access to the database

You can use the **dbaccess** command to limit which CMS logins have ODBC or JDBC access to the CMS database. The CMS database has “open access” permissions as a standard feature that allows any CMS login permission. By connecting to the CMS server via ODBC or JDBC, you can view any CMS table. No action is required if all CMS logins are allowed open access to the CMS database.

The **dbaccess** command does not provide control to which tables the CMS login has access or to which ACD data the CMS login can view.

The process of setting the secure database access is done in two parts:

1. First, all CMS login ids that are allowed CMS database access must be members of the RHEL group dbaccess.
2. Second, you must execute the **dbaccess** option of the **cmsadm** command to control which CMS logins have access to the CMS database.

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.

For detailed procedures about adding CMS logins to the dbaccess group, see the section “Using dbaccess” in *Maintaining and Troubleshooting Avaya Call Management System*.

Chapter 7: Resources

Documentation

CMS and CMS Supervisor documents

Title	Description	Audience
Overview		
Avaya Call Management System Overview and Specification	Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	All users
Installation and maintenance		
Deploying Avaya Call Management System	Describes how to install and configure CMS in a virtualized VMware or KVM environment.	Implementation engineers, administrators
Deploying Avaya Call Management System in an Infrastructure as a Service Environment	Describes how to deploy CMS in an Amazon Web Services or Google Cloud Platform environment.	Implementation engineers, administrators
Maintaining and Troubleshooting Avaya Call Management System	Describes how to configure, maintain, and troubleshoot CMS.	Administrators, support personnel
Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting	Describes how to connect and administer the Automatic Call Distribution (ACD) systems used by CMS.	Administrators, installation personnel, support personnel
Avaya Call Management System High Availability Connectivity, Upgrade and Administration	Describes how to connect to HA servers and upgrade to HA.	Administrators, installation personnel, software specialists involved with HA
Using Avaya Call Management System High Availability and Admin-Sync	Describes how to install and maintain your CMS High Availability (HA) system.	Administrators, support personnel
Upgrading		

Table continues…

Title	Description	Audience
Upgrading Avaya Call Management System	Describes the procedures required to upgrade to a new CMS release. This document is focused on full software or platform upgrades.	System administrators, implementation engineers
Avaya Call Management System Base Load Upgrade	Describes how to perform a simplified base load upgrade. You can perform a base load upgrade within a CMS release or for other approved scenarios. Not all releases support base load upgrades.	System administrators, implementation engineers
Administration		
Administering Avaya Call Management System	Provides instructions on administering a call center using CMS Supervisor.	Avaya support personnel, Administrators
Avaya Call Management System Call History Interface	Describes the format of the Call History data files and how to transfer these files to another computer.	Administrators, supervisors
Using ODBC and JDBC with Avaya Call Management System	Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Administrators, support personnel
Avaya Call Management System Database Items and Calculations	Describes each database item and calculation that CMS tracks and how CMS calculates the values displayed on CMS reports and CMS Supervisor reports.	Administrators, support personnel
Avaya Call Management System Custom Reports	Describes how to design and create custom reports in CMS.	Administrators, report designers
Avaya Call Management System Security	Describes how to implement security features in CMS.	Administrators, support personnel
CMS Supervisor		
Avaya CMS Supervisor Clients Installation and Getting Started	Describes how to install and configure CMS Supervisor.	Implementation engineers, system administrators
Avaya CMS Supervisor Reports	Describes how to use CMS Supervisor reports.	Supervisors, administrators
Avaya CMS Supervisor Report Designer	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Supervisors, administrators

Avaya Solutions Platform Documents

Title	Description	Audience
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform server	All users

Table continues…

Title	Description	Audience
Installing the Avaya Solutions Platform 130 Series	Describes how to install Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel
Maintaining and Troubleshooting Avaya Solutions Platform 130 Series	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.

- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A: Configuring Microsoft Azure for enterprise login authentication

About this task

You can configure Microsoft Azure to integrate with CMS to enable enterprise login authentication. You must configure Microsoft Azure to add a single-page application for the CMS Supervisor Web Client. Additionally, you must set the redirect value to match the CMS Supervisor Web Client URL configured on the CMS system.

Note:

The following sample procedure illustrates how to configure Microsoft Azure to enable enterprise login authentication for CMS.

Procedure

1. Log in to the Microsoft Azure portal.
2. Perform the steps to register a single-page application (SPA). For more information about registering a single-page application in the Microsoft identity platform, see https://docs.microsoft.com/en-us/azure/active-directory/develop/scenario-spa-app-registration#create-the-app-registration.

   Note:

   When your application registration completes, note the Application (client) ID and Directory (tenant) ID. You require these values later to configure CMS.
3. Configure the platform settings. This includes setting the Redirect URI to specify where the Microsoft identity platform should redirect the client. For more information, see https://docs.microsoft.com/en-us/azure/active-directory/develop/scenario-spa-app-registration#redirect-uri-msaljs-20-with-auth-code-flow.

   Note:

   - When configuring the single-page application settings, ensure that you specify the redirect URI and front-channel logout URL. These values are required for configuring the CMS `login.properties` file used for the single-page application. Additionally,

ensure that you see the message "Your Redirect URI is eligible for the Authorization Code Flow with PKCE" below the **Grant Types** section.

- In the **Implicit Grant and Hybrid Flows** section, ensure that the check boxes to select tokens are clear.

4. After completing the platform configuration, ensure that the `User.Read` permission of type *Delegated* exists in Azure for the application. You can view the list of API permissions by clicking **API permissions** in the left menu. If the Admin Consent column indicates *No*, grant admin consent by clicking **Grant admin consent**.

Next steps

You can now proceed with the steps to configure CMS.

Index

L

M

N

O

P

R

S

T

U

V

W