# Maintaining and Troubleshooting Avaya Call Management System

Release 21.0
Issue 3
July 2025

# Notices

© 2026 Avaya LLC. All Rights Reserved.

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.

© 2020-2025, Avaya LLC
All Rights Reserved.

**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** ..... 9
Purpose ..... 9
Change history ..... 9
**Chapter 2: Supported platforms and packages** ..... 10
Prerequisites ..... 10
Supported hardware platforms ..... 10
Supported software packages ..... 10
**Chapter 3: Configuring CMS software** ..... 12
Prerequisites ..... 12
Setting up CMS data storage parameters ..... 12
To modify CMS data storage parameters ..... 12
Assigning passwords to the default CMS login IDs ..... 14
Configuring the standard CMS options ..... 15
Prerequisites ..... 15
About the configuration methods ..... 15
Configuring CMS interactively ..... 16
Configuring CMS using a flat file ..... 20
Creating the flat file ..... 20
Using the flat file ..... 21
**Chapter 4: Installing and configuring optional software** ..... 23
Configuring the ODBC and JDBC server software ..... 23
Setting up LAN connections ..... 23
Prerequisites ..... 23
Editing the /etc/hosts file ..... 24
IPv6 Support ..... 24
Installing the Forecasting package ..... 25
Prerequisites ..... 27
Installing the External Call History package ..... 27
Installing the LDAP authentication package ..... 31
Installing an LDAP encryption certificate ..... 31
Installing the LDAP feature package on CMS ..... 32
Creating and migrating CMS users with LDAP authentication ..... 35
Managing LDAP authenticated users in CMS ..... 37
Adding a secondary IP address to an ACD ..... 37
To add a secondary IP address while adding a new ACD ..... 38
Activating the CMS Supervisor Web Client software ..... 38
Starting the Web Client software ..... 39
Generating a certificate for the Web Client server ..... 39
Installing the root certificate for the Web Client software ..... 40

Configuring EASG ..... 40
Setting up the Alarm Origination Manager ..... 41
Prerequisites ..... 42
Setting up AOM configuration for SNMP alarming ..... 42
Configuring AOM ..... 42
Configuring an Alarm Destination ..... 43
Configuring an SNMP User ..... 45
Configuring an Alarm ID ..... 48
Configuring a Customer ID ..... 49
Sending an AOM Test Alarm ..... 49
Clearing SNMP Alarms ..... 50
CMS SNMP alarm information ..... 51
Locating the CMS-MIB.txt file ..... 56
Configuring an Alarm Destination ..... 56
Configuring an Alarm ID ..... 58
Sending an AOM Test Alarm ..... 58
Setting the Informix configuration parameters for CMS ..... 59
**Chapter 5: Maintaining CMS** ..... 60
Using the CMSADM menu ..... 60
CMSADM menu functions ..... 60
Accessing the CMSADM menu ..... 61
Defining a new ACD (acd_create) ..... 61
Removing an ACD (acd_remove) ..... 62
Backing up the file system (backup) ..... 63
Installing feature packages (pkg_install) ..... 64
Removing feature packages (pkg_remove) ..... 64
Turning a feature package on/off (run_pkg) ..... 65
Turning IDS on/off (run_ids) ..... 66
Turning CMS on/off (run_cms) ..... 66
Switching password aging on/off (passwd_age) ..... 67
Controlling ODBC/JDBC database access (dbaccess) ..... 68
Configuring a feature package (config_pkg) ..... 70
Using the CMSSVC menu ..... 70
Accessing the CMSSVC menu ..... 70
Displaying the authorisation status (auth_display) ..... 71
Setting the WebLM server address (weblm_set) ..... 72
Turning IDS on/off (run_ids) ..... 72
Turning CMS on/off (run_cms) ..... 73
Running the CMS initial configuration (setup) ..... 73
Display the ACD switch info (swinfo) ..... 73
Changing the ACD switch options (swsetup) ..... 74
Uninstalling CMS (uninstall) ..... 75
Editing the CMS security options (security) ..... 76

Maintaining WebLM licenses ... 82
Activating the license for a CMS server ... 82
Installing a license file on a WebLM server ... 83
Managing alarms and error logs ... 84
Warning message in the License Error mode ... 85
Backing up and restoring WebLM ... 85
Upgrading to WebLM ... 85
Managing personal data in CMS ... 86
Deleting phone numbers from CMS ... 86
Personal data log files ... 87
Configuring the encryption passphrase ... 87
Updating the LDAP authentication package configuration ... 90
LDAP authentication configuration ... 90
Installing an LDAP encryption certificate ... 90
Updating the LDAP authentication configuration ... 91
Removing the LDAP authentication package ... 93
Backing up data ... 94
CMSADM backup ... 95
When to do a CMSADM backup ... 95
When to do a maintenance backup ... 96
Data space requirements for CMS backups ... 96
Backing up CMS to a USB storage device ... 98
Backing up CMS to a network mounting point ... 104
Backup encryption and other options ... 118
Powering off CMS on a virtual machine ... 118
Starting up CMS on a virtual machine ... 119
Adding disk storage space to a CMS virtual machine ... 119
Adding additional disk storage to a VMware server ... 120
Adding disk storage space to a KVM server ... 121
Attaching the newly added disks to the Informix database ... 121
Changing the system date and time ... 122
Checking the RHEL system date and time ... 122
Setting the system date and time ... 122
Changing the time zone ... 123
Working with CMS patches ... 123
CMS patch requirements ... 123
Installing CMS patches ... 124
Removing CMS patches ... 125
Configuring password aging ... 125
Excluding a user from password aging ... 126
Switching password aging on/off (passwd_age) ... 126
Checking user password status ... 127
Removing a user from the aging exclusion file ... 128

Setting a different password aging for a user ..... 129
Maintaining the chkDisks crontab ..... 130
Verifying chkDisks ..... 130
Changing the chkDisks run time ..... 130
Canceling chkDisks ..... 130
About the Archiving process ..... 131
About time zone archiving with additional time zones ..... 131
**Chapter 6: Recovering a CMS server** ..... 133
Back up CMS ..... 133
Deploy a new CMS server ..... 133
Restore CMS setup using a CMSADM backup ..... 133
Restore CMS data using a CMS Maintenance restore ..... 135
Data restore requirements ..... 135
Before restoring data ..... 135
Restoring data from a full maintenance backup ..... 136
Restoring data from a full and incremental maintenance backup ..... 137
Restoring data using a binary backup ..... 139
Using tapeless migration ..... 141
**Chapter 7: Additional restore procedures** ..... 142
Recovering a mirrored system after disk failure ..... 142
Prerequisites P195 ..... 142
Doing a CMSADM restore of a system ..... 142
Prerequisites ..... 143
Restoring a system from a CMSADM backup ..... 143
Restoring a system without a CMSADM or system backup ..... 154
Restoring specific files from the CMSADM backup ..... 154
Restore CMS data using a CMS Maintenance restore ..... 155
Data restore requirements ..... 155
Restoring data from a full maintenance backup ..... 156
Restoring data from a full and incremental maintenance backup ..... 157
Restoring data using a binary backup ..... 159
Using tapeless migration ..... 161
**Chapter 8: Troubleshooting** ..... 162
Determining your CMS version ..... 162
Recognizing new hardware devices ..... 162
Tracking changes to password aging ..... 163
Tracking changes to password aging ..... 163
Passwords of excluded users age ..... 163
CMS logs ..... 163
CMS error logs ..... 164
Audit logging of administrative actions ..... 165
Checking installed software packages ..... 166
Diagnosing a machine panic ..... 166

Common problems using the disc drive ..... 167
Verifying that the system can read a disc..... 167
Disc drive fails to open ..... 167
Removing the CMS package fails ..... 168
CMS installation fails..... 168
CMSADM backup problems..... 168
System messages ..... 169
RAID for CMS..... 170
Troubleshooting problems with disk drives..... 170
Common error messages..... 171
Troubleshooting reports..... 173
Report Query Status..... 173
Report database updates..... 175
Location and configuration of the updatelog..... 175
Troubleshooting an empty or incomplete report..... 176
Troubleshooting Workmode status icon on Integrated Reports..... 176
How to determine whether the archiver has run ..... 176
Troubleshooting Visual Basic Errors..... 178
Troubleshooting LDAP server configuration issues..... 183
LDAP server log files..... 183
Verifying LDAP server connectivity on a non-encrypted connection..... 183
Troubleshooting LDAP server connectivity on an encrypted connection..... 185
Dictionary management..... 187
**Chapter 9: Resources**..... 188
Documentation..... 188
Finding documents on the Avaya Support website..... 190
Avaya Documentation Center navigation..... 190
Viewing Avaya Mentor videos..... 192
Support..... 192
Using the Avaya InSite Knowledge Base..... 192
**Appendix A: Example of a flat file**..... 194

# Chapter 1: Introduction

## Purpose

The document describes how to configure, maintain, and troubleshoot Avaya Call Management System software. It is intended for support personnel and contact center administrators.

Users of this document must be familiar with CMS and the Red Hat Enterprise Linux (RHEL) operating system.

## Change history

The following table outlines the key changes in this document for Release 21.x:

| Issue | Date | Summary of changes |
|---|---|---|
| 3 | July 2025 | • Add process for adding additional storage on KVM virtual machines. |
| 2 | November 2024 | • Corrected the information about generating a certificate for the Web Client server.<br>• Updated password aging information.<br>• Minor rephrasing changes. |
| 1 | June 2024 | • Remove outdated `cmsweb.jks` references in commands.<br>• Updated the Calculating data space requirements for CMS full maintenance backups on page 97 to remove obsolete references.<br>• Revised backup information and indicated that you can access the backup utility from the command line interface or an unattended cron job.<br>• Added Backup encryption and other options on page 118.<br>• Revised server information in Adding disk storage space to a CMS virtual machine on page 119.<br>• Added CMS logs on page 163.<br>• Added Dictionary management on page 187.<br>• Removed outdated certificate management and hardware information.<br>• Revised troubleshooting information. |

# Chapter 2: Supported platforms and packages

This chapter lists the hardware platforms and software that is supported by Avaya Call Management System.

## Prerequisites

Before you use any procedures in this document, confirm that a valid CMS license file is installed on a WebLM Release 8.0 or later server. For more information, see:

## Supported hardware platforms

CMS is supported on the following platforms:

- Avaya Solutions Platform ASP 130 R6 servers.
- Customer-provided VMware servers.
- Customer-provided KVM servers.
- Customer-provided Amazon Web Services (AWS) servers.
- Customer-provided Google Cloud Platform (GCP) servers.

**Important:**

CMS no longer supports hardware-only installations and upgrades.

## Supported software packages

CMS uses the following software:

- CMS server software
- CMS Supplemental Services

- Informix IDS
- Informix ESQL SDK
- Informix ILS
- ODBC and JDBC

# Chapter 3: Configuring CMS software

The CMS software is configured when a system is first installed or when a system is upgrading. Use the procedures in this chapter to make changes to the CMS configuration.

## Prerequisites

Before you install any of the CMS packages, verify that you are logged on as root at the console.

## Setting up CMS data storage parameters

This section describes how Avaya Services personnel modify specific data storage parameters on the CMS server. These storage parameters affect the operation of the CMS software.

**Important:**

Throughout the setup, you are prompted to enter values that are specific to the system being installed. These values differ between switch releases.

For each question, an appropriate range of values is displayed. These values represent the limits of each range.

## To modify CMS data storage parameters

### Procedure

1. Change to the CMS installation directory by entering:`cd /cms/install/cms_install`
2. Enter:`vi storage.def`

**Note:**

The `storage.def` file contains the data storage parameters. CMS is installed with a set of standard default values.

If you delete or damage the storage.def file, you can find a copy of this file (storage.skl) in the same directory.The default storage parameters are listed in the Default CMS in

the order in which they appear in the storage.def file. The data storage parameters are documented in the Avaya Aura® Communication Manager System Capacities Table.

**Table 1: Default CMS data storage parameters table:**

| Parameter | Default |
|---|---|
| Intrahour interval (15, 30, 60 minutes): | 30 |
| Week start day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday): | Sunday |
| Week end day (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday): | Saturday |
| Daily start time (regular time): | 12:00 AM |
| Daily stop time (data will be collected for seconds of last minute): | 11:59 PM |
| Number of agent login/logout records: | 10000 |
| Number of agent trace records: | 10000 |
| Number of call records: | 0 |
| Number of exceptions records: | 250 |
| # Days of intrahour for splits (1-370): | 62 |
| # Days of daily splits (1-1825): | 387 |
| # Weeks of weekly splits (1-520): | 53 |
| # Months of monthly splits (1-120): | 13 |
| # Days of intrahour for agents (1-370): | 62 |
| # Days of daily agents (1-1825): | 387 |
| # Weeks of weekly agents (1-520): | 53 |
| # Months of monthly agents (1-120): | 13 |
| # Days of intrahour for trunk groups (1-370): | 62 |
| # Days of daily trunk groups (1-1825): | 387 |
| # Weeks of weekly trunk groups (1-520): | 53 |
| # Months of monthly trunk groups (1-120): | 13 |
| # Days of intrahour for trunks (1-370): | 62 |
| # Days of daily trunks (1-1825): | 387 |
| # Weeks of weekly trunks (1-520): | 53 |
| # Months of monthly trunks (1-120): | 13 |
| # Days of intrahour for call work codes (1-370): | 62 |
| # Days of daily call work codes (1-1825): | 0 |
| # Weeks of weekly call work codes (1-520): | 0 |
| # Months of monthly call work codes (1-120): | 0 |
| # Days of intrahour for vectors (1-370): | 62 |

*Table continues…*

| Parameter | Default |
|---|---|
| # Days of daily vectors (1-1825): | 387 |
| # Weeks of weekly vectors (1-520): | 53 |
| # Months of monthly vectors (1-120): | 13 |
| # Days of intrahour for VDNs (1-370): | 62 |
| # Days of daily VDNs (1-1825): | 387 |
| # Weeks of weekly VDNs (1-520): | 53 |
| # Months of monthly VDNs (1-120): | 13 |

3. Review the default data storage values for each authorized ACD. The default values are found on the line immediately below each storage parameter
4. Enter the values determined by the account executive, system consultant, and design center. These values are based on the customer configuration.
5. Press `Esc`. Then enter: `:wq!`

   The system saves and closes the file.

   After the CMS software is running, the system administrator can change the data storage parameters using the Data Storage Allocation window and the Storage Intervals window. Both Windows are accessed from the CMS System Setup menu.

# Assigning passwords to the default CMS login IDs

## Procedure

1. Enter :`passwd cms`

   The system displays the following message

   ```
   New password:
   ```

2. Enter the password for the Avaya CMS login.

   The system displays the following message:

   ```
   Re-enter new password:
   ```

3. Re-enter the password for the Avaya CMS login.

   The system displays the following message:

   ```
   passwd: password successfully changed for cms
   ```

4. Assign a password for the Avaya `cmssvc` login, enter:`passwd cmssvc`

   The system displays the following message:

   ```
   New password:
   ```

5. Enter the password for the Avaya `cmssvc` login.

The system displays the following message:

```
Re-enter new password:
```

6. Re-enter the password for the Avaya `cmssvc` login.

   The system displays the following message:

   ```
   passwd: password successfully changed for cmssvc
   ```

# Configuring the standard CMS options

The CMS software provides monitoring and recording of ACD calls and agents handling these calls, and the use of Vector Directory Numbers (VDNs) for these calls to measure call center performance

# Prerequisites

Before you configure the CMS software, do the following tasks:

- Verify that you are logged on as root.

  **Important:**

  You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

- Verify that if TCP/IP is being used to connect to an ACD, the switch/LAN setup is done.
- Verify that all file systems are mounted.

# About the configuration methods

You can choose either of the following ways to configure the CMS software:

- If you use the interactive option, the program automatically prompts you for the necessary information to configure the CMS software.
- If you use the flat file option, you edit a system flat file that contains the necessary information to set up the CMS software. When you execute the install program, the program runs in the background and uses the flat file data to configure CMS.

**Caution:**

Using the CMS setup option of the cmssvc command erases all previous setup information. Ensure that you have any old setup information on record when you run the setup option.

# Configuring CMS interactively

## Procedure

1. Enter: `cmssvc`

   **Note:**

   If you are executing the cmssvc command for the first time, the system does not display the menu. Instead, the system automatically prompts for WebLM setup, EASG setup, and encryption passphrase setup.

   The system displays the Avaya Call Management System Services Menu.

2. Enter the option number for the `setup` command.

   **Caution:**

   If setup has been done previously, the system displays the following message:

   ```
   Warning!!! Setup has already been performed.
   Running this command will remove all CMS data in the database.
   Do you wish to proceed and re-configure CMS? (y/n): (default: n)
   ```

   a. If CMS is turned on, the system displays the following message and returns to the command prompt.

   ```
   CMS needs to be turned off before invoking this command.
   ```

   b. If is turned off, the system displays options for the set up type.

3. Select the option for the terminal.

   When the `cmssvc` setup command is running, no other CMSADM or cmssvc commands are allowed. Any attempt to run other CMSADM or `cmssvc` commands will be rejected, and the system will display the error message Please try later, setup is active.

   If system setup has already been done, the program responds:

   ```
   Warning!!! Setup has already been performed.
   Running this command will remove all CMS data in the database.
   Do you wish to proceed and re-configure CMS? (y/n): (default: n)
   ```

   If the warning message is displayed, do one of the following actions:

   Enter `N` to exit the setup.

   Enter `Y` to continue with the setup.

   The system displays the following message:

   ```
   Select the language for this server:
   All languages are ISO Latin except Japanese. Selection of the
   server language assumes that existing customer data is compatible. (Upgrade from
   any ISO Latin language to any ISO Latin language or from Japanese to Japanese is
   supported).
   1) English
   2) Dutch
   3) French
   4) German
   ```

```
5) Italian
6) Portuguese
7) Spanish
8) Japanese
Enter choice (1-8): (default: 1)
```

4. Enter the number for the language to be used on this system.

   The system displays the following options if a flat file exists; otherwise, this menu is not displayed:

   ```
   The input will be read from
   1) The terminal
   2) a flat file
   Enter choice 1 or 2:
   ```

5. Enter the number associated with the terminal option. The system initializes the customer CMS data. This can take up to 15 minutes. When finished, the system displays the following message:

```
## Initializing Customer CMS data . . .
.........................
Customer CMS data successfully initialized.
Creating database tables
.......
Enter a name for this UNIX system (up to 256 characters): (default: cms3)
```

6. Enter the host name of the CMS server. This name was assigned during networking setup and is used by Avaya Services to maintain and identify this specific system.

   The system displays the following message:

   ```
   Select the type of backup device you are using
   1) Tape
   2) Other
   Enter choice (1-2):
   ```

   **Note:**

   Avaya Solutions Platform servers do not have a tape drive option.

   The system displays the following message:

   ```
   Enter the default backup device path: (default: /dev/null)
   ```

   **Warning:**

   You cannot do backups to `/dev/null`. The `/dev/null` device path allows customers who do not have a backup device to continue configuring CMS.

   The `/dev/null` device path is not an option if type **Other** is selected. The CMS administrator needs to provide the path used for type **Other**.

7. Enter the default backup device path.

   The system displays the following message:

   ```
   Enter number of ACDs being administered (1-8): (default: 2)
   ```

8. Enter the number of ACDs (Communication Manager systems) to be administered. This number may be less than the number of ACDs authorized.

The system displays the following message:

```
Information for ACD 1
Enter switch name (up to 20 characters):
```

9. Enter the name for the Communication Managersystem that is associated with ACD 1. The system displays a list of Communication Manager releases.
10. Enter the number that represents the Communication Manager releases that is associated with the ACD.

    **Important:**

    To administer an encrypted link between CMS and a Communication Manager system, you must use the CM 8.1.2+ Secured option on CMS setup and the R19.1+ (secured) option on Communication Manager. If you do not want an encrypted link, use the Communication Mgr 8.x option on CMS and R19.0 onCommunication Manager.

    The system displays the following message:

    ```
    Enter the local port assigned to switch (1-64):
    ```

    **Note:**

    The standard CMS provisioning procedure is to set the local and remote port assignments equal to the switch processor channel assignment.

    For example, for switch processor channel 2, the remote and local port assignments would both be set to a value of 2.

11. Enter the local port or channel number on the switch. The system displays the following message:

    ```
    Enter the remote port assigned to switch (1-64):
    ```

12. Enter the remote port or channel number on the switch. The system displays the following message:

    ```
    Enter switch host name or IP Address:
    ```

13. Enter the host name or IP address of the Communication Manager system that is connected to this ACD.

    **Note:**

    If you enter a host name that has not been added to the computer's /etc/hosts file, the system displays the following message:

    ```
    Switch_name has not been administered in a DNS or
    /etc/hosts file. The DNS or /etc/hosts file must be
    corrected or the link to the switch will not work.
    ```

    The system displays the following message:

    ```
    Enter switch TCP port number (minimum-maximum):(default: 5001)
    ```

14. Press `Enter` to use the default TCP port number.

**Note:**

This number must match the port number administered on the switch.The system displays the following message:

```
Number of splits/skills (0-Maximum): (default: 350)
```

15. Enter the number of splits/skills in this ACD. The system displays the following message:

```
Total split/skill members, summed over all splits/skills
(0-Maximum):(default 3500)
```

16. Enter the maximum number of split/skill members that will be logged into this ACD simultaneously, considering shift overlap. If it is not possible to sum the number of splits/skills for each agent, you can determine the capacity that is needed by multiplying the total number of agents by the average number of splits/skills per agent.

    The system displays the following message:

```
Number of trunk groups(0-maximum):(default 350)
```

17. Enter the number of trunk groups that are associated with this ACD. The system displays the following message:

```
Number of trunks (0-maximum):(default 1000)
```

18. Enter the number of trunks associated with this ACD. The system displays the following message:

```
Number of unmeasured facilities (0-maximum):(default: 500)
```

19. Enter the number of unmeasured trunk facilities that are associated with this ACD.

    **Note:**

    The recommended assignment per ACD for unmeasured facilities is 50% of the measured trunks.

    If the Communication Manager system supports call work codes, the system displays the following message:

```
Number of call work codes (minumum-maximum):(default 750)
```

20. Enter the number of call work codes.If vectoring is enabled, that is if a`Y` was entered in Step 12, the system displays the following message.

```
Enter number of vectors (0-maximum):(default 350)
```

21. Enter the number of vectors. The system displays the following message:

```
Enter number of VDNs (0-maximum):(default 2000)
```

22. Enter the number of VDNs. If you have another ACD to define, the setup program repeats starting at step 10. After you define the last ACD, the system displays the following message:

```
Updating database.
Creating database tables
.......
Computing space requirements and file system space
availability.
Setup completed successfully.
```

**Note:**

If the setup determines that you do not have enough file space, the system displays the following warning message:

```
Failed to find sufficient file space for CMS data.
WARNING: You do not currently have sufficient file space for your
existing CMS data. At this point you should turn on CMS, go to the
"Data Storage Allocation" screen, verify/modify the
administration, and go to the "Free Space Allocation" screen and
verify your available free space.
Setup completed with warnings.
```

23. To verify that the installation completed successfully, enter: `tail /cms/install/logdir/admin.log`.

    All failure messages are logged in this file. The CMS software is successfully set up when the system displays a message similar to the following: `Setup completed successfully <date/time>`

24. Do one of the following actions:

    If you are not installing any other feature packages, do the following procedure:

    - Enter: `cmssvc`. The system displays the **Avaya Call Management System Services** Menu.
    - Enter the number associated with the **run_cms** option.
    - Enter the number associated with the **Turn on CMS** option.

# Configuring CMS using a flat file

To configure CMS using a flat file, you must edit a copy of the `cms.inst.skl` file and start the install program.

**Important:**

This procedure is not necessary if you already configured CMS interactively.

# Creating the flat file

## Procedure

1. Change to the CMS installation directory by entering: `cd /cms/install/cms_install`
2. Make a copy of the CMS installation file by entering: `cp cms.inst.skl cms.install`
3. Change permissions on the copied CMS installation file by entering: `chmod 644 cms.install`

4. Edit the copied CMS installation file by entering: `vi cms.install`

   The file contains a series of questions and value ranges for the ACD configuration. Enter the appropriate values for your configuration. The entries must be added on the blank lines after each question.

   **Caution:**

   Use the computer's hostname for the system name. The computer's hostname was assigned during network setup.

5. Press `Esc`.
6. Enter: `:wq!`.

   The system saves and closes the file.

# Using the flat file

## Procedure

1. Enter cd / to change to the directory
2. Enter: `cmssvc`

   **Note:**

   If you are executing the cmssvc command for the first time, the system does not display the menu. Instead, the system automatically prompts for WebLM setup, EASG setup, and encryption passphrase setup. The system displays the **Avaya Call Management System Services** Menu.

3. Enter the number associated with the **setup** option.

   **Caution:**

   If setup has been done previously, the system displays the following message:

   ```
   Warning!!! Setup has already been performed.
   Running this command will remove all CMS data in the database.
   Do you wish to proceed and re-configure CMS? (y/n): (default: n)
   ```

4. Enter: `Y`. The system displays the following message:

   ```
   Select the language for this server:
   All languages are ISO Latin except Japanese. Selection of the
   server language assumes that existing customer data is compatible.
   (Upgrade from any ISO Latin language to any ISO Latin language or
   from Japanese to Japanese is supported).
   1) English
   2) Dutch
   3) French
   4) German
   5) Italian
   6) Portuguese
   7) Spanish
   ```

```
8) Japanese
Enter choice (1-8): (default: 1)
```

5. Enter the number associated with the language that is used on the system.The system displays the following message:

```
The input will be read from
1) the terminal
2) a flat file
Enter choice (1-2):
```

6. Enter the number associated with the **flat file** option. The system displays the following message:

```
*** The rest of this command is running in the background ***
```

7. Verify that the installation completed successfully by entering: `tail -f /cms/install/logdir/admin.log`. The `-f` option in the tail command updates the console as messages are written to the admin.log file. All failure messages are logged in this file. The CMS software is successfully set up when you see a message similar to the following:

```
Setup completed successfully <date/time>
```

   You can edit this file and add comments about the packages that were installed or authorized.

8. Press `Delete` to exit the tail `-f` command.
9. Choose one of the following:
   - If you are not installing any other feature packages, do the following to turn on the CMS software:
     a. Enter: `cmssvc`. The system displays the Avaya Call Management System Services Menu.
     b. Enter the number associated with the **run_cms** option.
     c. Enter the number associated with the **Turn on CMS** option.

**Important:**

If no additional configuration of the CMS software is needed, see Setting the Informix configuration parameters for CMS on page 83.

# Chapter 4: Installing and configuring optional software

## Configuring the ODBC and JDBC server software

This document describes using Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) to access data in the CMS database.

ODBC and JDBC databases enable you to:

- Directly access CMS data from your software applications.
- Use the data in spreadsheet programs and other applications.
- Generate reports using data from multiple CMS sites.

For more information on ODBC and JDBC database, see: *Using ODBC and JDBC with Avaya Call Management System*.

## Setting up LAN connections

This section describes how to set up a network connection to a LAN-enabled switch and other CMS server peripherals. For more information about LAN switch configurations, see:*Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting*

### Prerequisites

Before you begin setting up the network for LAN connections, do the following tasks:

- Verify that you are logged on as root.

  **Important:**

  You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

- Verify that the CMS software is turned off and the IDS software is on.
- Verify that all file systems are mounted.
- Verify that Avaya Aura® Communication Manager 6.0 or later is installed.

# Editing the /etc/hosts file

## Procedure

1. Enter: `vi /etc/hosts`

   **Important:**

   The items in this file must be separated by tabs, not spaces, and any comments must begin with a #. The entry for `loghost` must remain on line four and the entry for `loghost` must remain online.

   The `loghost` line should contain the CMS server's:

   - IP Address
   - Hostname
   - Hostname fully qualified domain name
   - `loghost`

   The fully qualified domain name is either the customer domain name or the default entry `tempdomain.net`

   ```
   #
   # Internet host table
   #
   127.0.0.1 localhost
   192.168.2.1 cms cms.tempdomain.net loghost
   ```

2. Add a new line to this file for each ethernet card that is installed in this computer using TCP/IP. This example shows the recommended default IP addressing scheme for a closed network.

   ```
   #
   # Internet host table
   #
   127.0.0.1 localhost
   192.168.2.1 cms cms.tempdomain.net loghost
   192.168.2.2 switch
   192.168.2.103 router
   ```

   **Note:**

   Only the primary network card needs the fully qualified domain name.

3. Press `Esc`. Then enter: `:wq!`

   The system saves and closes the file.

# IPv6 Support

## Procedure

1. Edit `/etc/hosts` and add a line with the IPv6 host name.

   For example,

   ```
   9876:543g:FGHI:5431:ywxz:1a2b:0032:A0Z3 cms_ipv6_1
   ```

Press `Esc`. Then `enter`. The system saves and closes the file.

2. IPv6 SupportConfigure the /etc/sysconfig/network-scripts/ifcfg-ethX file to support IPv6 by entering:`vi /etc/sysconfig/network-scripts/ifcfg-ethX`.

   Where `ifcfg-ethX` is the network interface, and X is the instance of the network interface.

   Append the following options to support IPv6. For example,

   ```
   IPV6INIT=yes
   IPV6ADDR=9876:543g:FGHI:5431:ywxz:1a2b:0032:A0Z3
   IPV6_DEFAULTGW=1234:f567:ABCD:0001:aBcD:9876:efGH:1111
   ```

   ```
   DEVICE=eth1
   ONBOOT=yes
   BOOTPROTO=static
   HWADDR=01:02:03:04:05:06
   IPADDR=192.168.2.1
   NETMASK=255.255.255.255
   IPV6INIT=yes
   IPV6ADDR=9876:543g:FGHI:5431:ywxz:1a2b:0032:A0Z3
   IPV6_DEFAULTGW=1234:f567:ABCD:0001:aBcD:9876:efGH:1111
   ```

3. Edit the `/etc/sysconfig/network` file to support the IPv6 network interface by entering: `vi /etc/sysconfig/network`.

   Append the following option to support IPv6:

   ```
   NETWORKING_IPV6=yes
   ```

4. Configure the `/etc/sysconfig/network` file with the IPv6 host name you added to the /etc/hosts file. Enter the appropriate information for each item.

   ```
   NETWORKING=yes
   HOSTNAME=cms_ipv6_1
   GATEWAY=192.168.2.254
   NETWORKING_IPV6=yes
   ```

5. Press `Escape`. Then `enter`:`:wq!`
6. Edit the `/etc/sysconfig/network-scripts/route6-ethx` to define static IPv6 routes.

   ```
   vi /etc/sysconfig/network-scripts/route6-ethx
   ```

   Enter the IPv6 route information. For example,

   ```
   ::/32 via defd:ebne:ADJL:wxyz dev ethx
   ```

7. Press `Escape`. Then `enter`: `:wq!`

   The system saves and closes the file.

# Installing the Forecasting package

## Procedure

1. Enter: `cmssvc`

The system displays the **Avaya Call Management System Services** Menu.

2. Enter the number associated with the `auth_display` option. The system lists the current authorizations.
3. Verify that the system is authorized to install the Forecasting package.
4. Enter: `cmsadm`. The system displays the **Avaya Call Management System Administration** Menu.

   **Note:**

   Different options may be displayed in the **Avaya Call Management System Administration** Menu depending on the current version of CMS on your system.

5. Enter the number associated with the pkg_install option. The system displays the following message:

```
The CMS features that can be installed are
1) forecasting
2) external call history
3) multi-tenancy
4) Dual IP
5) LDAP authentication
Enter choice (1-3) or q to quit:
```

   **Note:**

   The `pkg_install` option menu displays only those feature packages that are not yet installed. The Forecasting package does not require the CMS software to be off during the installation. If Forecasting is added at a later date, the CMS software can be left on.

6. Enter the number that corresponds to the `forecasting` package. The system displays the following message:

```
Installation was successful
Forecasting package installed.
At this point you should go to the "Free Space Allocation Screen"
and verify that you have enough space for Forecasting on each ACD.
If there is not enough space allocated, then modify your existing
free space.
```

   If the installation fails, the system displays the following message:

```
Forecasting package installation failed.
```

7. If you are not installing any other feature packages, do the following to turn on the CMS software:
   a. Enter: `cmssvc`. The system displays the **Avaya Call Management System Services** Menu.
   b. Enter the number associated with the **run_cms** option.
   c. Enter the number associated with the **Turn on CMS** option.

8. Go to the Free Space Allocation window that is located in the CMS System Setup subsystem, verify that there is enough space for Forecasting on each ACD, and make any necessary modifications.

   For more information about Free Space Allocation, see *Administering Avaya Call Management System*.

9. Verify that the installation completed successfully by entering: `tail /cms/install/logdir/admin.log`.

   If the Forecasting package was successfully installed, the system displays the following message:

   ```
   ..
   Forecasting package installed (date/time)
   ```

   You can edit this file in order to add comments about the packages that were installed or authorized.

# Prerequisites

Before you begin the installation procedures, do the following tasks:

- Verify that you are logged on as root.

  **Important:**

  You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

- Verify that all file systems are mounted.

# Installing the External Call History package

## Before you begin

**Important:**

Once the External Call History package is installed, you can no longer access any call record data directly from the CMS software. For more information, see *Avaya Call Management System Call History Interface*.

## Procedure

1. Verify if :
   - A separate computer is available for the storage and reporting of call records.
   - The CMS software is off and the IDS software is on.
2. Enter: `cmssvc`. The system displays the **Avaya Call Management System Services** Menu.
3. Enter the number associated with the `auth_display` option.

   The system displays the current authorizations. The system can display different authorizations depending on the version of CMS on your system.

4. Verify that the system is authorized for the ECHI package.
5. Enter: `cmsadm`.
6. Enter the number associated with the `pkg_install` option. The system displays the following message:

```
The CMS features that can be installed are
1) forecasting
2) external call history
3) multi-tenancy
4) Dual IP
5) LDAP authentication
Enter choice (1-3) or q to quit:
```

**Note:**

The system displays only feature packages that are authorized but not yet installed.

7. Enter the number that corresponds to the ECHI package . The system displays the following message:

```
Enter full path of the program to transmit the external call
history files: (default: /cms/dc/chr/no_op.sh)
```

8. Press `Enter`.The system displays the following message:

```
Enter full path of the program to check the external call history
file transmission: (default: /cms/dc/chr/no_op.sh)
```

9. Press `Enter`.The system displays the following message:

```
Number of call segments to buffer for ACD xxxxx (0-99999):
```

10. Enter the number of call records to be held in the buffer if the Call History machine cannot accept the data. Repeat this step for each administered ACD .The system displays the following message:

```
Start ECH in the on or off state: (default off)
```

11. Select whether ECHI will start in the on or off state (default is off). If the receiving system has not yet been set up, the recommended state is off. ECHI can be turned on at a later date with the run_pkg option in the **Avaya Call Management System Administration** Menu. If the setup determines that you do not have enough file space, you get the following warning message:

```
Failed to find sufficient file space for CMS data.
WARNING: You do not currently have sufficient file space for your
existing CMS data. At this point you should turn on CMS, go to the
"Data Storage Allocation" screen, and verify/modify the
administration, or go to the "Free Allocation" screen and verify/
modify your existing free space.
External call history package installed with warnings.
```

12. Verify that the installation completed successfully by entering: `tail /cms/install/logdir/admin.log`. If the ECHI package was installed successfully, the system displays the following message:

```
External Call History package installed (date/time)
```

13. If you are not installing any other feature packages, do the following to turn on the CMS software:
    a. Enter: `cmssvc`. The system displays the **Avaya Call Management System Services** Menu.
    b. Enter the number associated with the **`run_cms`** option.
    c. Enter the number associated with the **Turn on CMS** option.

    For more information about the ECHI feature, see *Avaya Call Management System Call History Interface*.

## Installing the Multi-tenancy package

### Procedure

1. Enter: `cmssvc`. The system displays the **Avaya Call Management System Services** Menu.
2. Enter the number associated with the `auth_display` option.The system lists the current authorizations.
3. Enter: `cmsadm`. The system displays the **Avaya Call Management System Administration** Menu.

   **Note:**

   The system can display different options in the Avaya Call Management System Administration Menu depending on the current version of Avaya CMS on your system.
4. Enter the number associated with the `pkg_install` option. The system displays the following message:

```
The  features that can be installed are
1) forecasting
2) external call history
3) multi-tenancy
4) Dual IP
5) LDAP authentication
Enter choice (1-3) or q to quit:
```

   **Note:**

   The pkg_install option menu displays only those feature packages that are authorized but not yet installed. The Multi-tenancy package does not require the Avaya CMS software to be off during the installation. If Multi-tenancy is added at a later date, the Avaya CMS software can be left on.
5. Enter the number that corresponds to the `multi-tenancy` package. The system displays the following message:

```
Installation was successful
Multi-tenancy package installed.
```

   If the installation fails, the system displays the following message:

```
Multi-tenancy package installation failed.
```

6. If you are not installing any other feature packages, do the following to turn on the Avaya CMS software:
   a. Enter: `cmssvc`. The system displays the Avaya Call Management System Services Menu.
   b. Enter the number associated with the `run_cms` option.
   c. Enter the number associated with the **Turn on CMS** option.
7. Go to the Free Space Allocation window that is located in the Avaya CMS System Setup subsystem. Verify that there is enough space for Multi-tenancy and Data Summarization Time Zones on each ACD. Make any necessary modifications.You can optionally administer a second time zone for an ACD. For that second time zone, the Free Space Allocation feature automatically accounts for the second time zone.
8. Verify that the installation completed successfully. Enter: `tail /cms/install/logdir/admin.log`

   If the Forecasting package was successfully installed, the system displays the following message:

   ```
   Multi-tenancy package installed (date/time)
   ```

   You can edit this file in order to add comments about the packages that were installed or authorized.

## Installing the Dual IP package

### Before you begin

You must run the `cmssvc/setup` command in the Command Prompt before enabling the Dual IP feature on new Avaya Call Management System deployments. You can install the Dual IP feature immediately after completing an upgrade to your Avaya Call Management System.

To install the Dual IP feature perform the following steps:

### Procedure

1. Enter: `cmsadm`.

   The **Avaya Call Management System Administration** menu will be displayed.
2. Enter the number associated with the `pkg_install` option.

   The application will display the list of CMS features that must be installed.

   ```
   The CMS features that can be installed are
   1) forecasting
   2) external call history
   3) multi-tenancy
   4) Dual IP
   5) LDAP authentication
   Enter choice (1-3) or q to quit:
   ```
3. Enter the number associated with the `Dual IP` option.The application returns a message to confirm that the Dual IP package is installed.

   ```
   Dual IP package installed.
   ```

# Installing the LDAP authentication package

You can manage users in CMS using Active Directory (AD) integration. It supports Active Directory for the Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, and 2019 versions. The AD integration connects to one AD system at once. The AD integration does not support Azure AD. Activating LDAP integration will not change the way you use CMS.

LDAP integration streamlines user login for CMS using:

Authentication: You can directly authenticate against the configured LDAP server during login.

Password Management: The Password Management eliminates the need to manage CMS user passwords through Avaya Services.

The CMS allows you to manage both traditional Linux users and those authenticated through LDAP.

When you activate LDAP, the LDAP system upgrades the existing CMS User Data screen.

This new interface lets you identify and manage LDAP-authenticated users alongside traditional ones.

The CMS users can log on using all CMS interfaces, including,

- CMS Supervisor Web Client
- CMS Supervisor PC Client
- CMS ASCII

The LDAP authentication feature package offers an optional layer of security. You can choose to encrypt the connection between CMS and the Active Directory (AD) server. This encryption helps protect sensitive user data from being exposed during communication over the LDAP protocol.

**Note:**

The CMS user ID maps to the Active Directory user or person **objectClass:sAMAccountName** field. The CMS user IDs can be up to 31 characters long. When using LDAP, user IDs are limited to 20 characters to match Active Directory's s **AMAccountName** field. Keep the LDAP user IDs under 20 characters to avoid login problems.

You must verify that the user name is configured in a user or person objectClass and that the user name is in the **sAMAccountName** field.

The installation log file for LDAP is found in the CMS security log located at: `/cms/install/logdir/security/cms_sec.log`.

# Installing an LDAP encryption certificate

### About this task

If you plan to use encryption over the LDAP connection, you must export the Active Directory certificate from the Windows Active Directory server. This procedure exports the Certificate Authority Active Directory certificate and installs the certificate on the CMS server.

**Important:**

If you are not encrypting the LDAP connection, you can skip this procedure.

### Procedure

1. Log on to Windows as an administrator on the LDAP AD server.
2. Open a command window.
3. Run the following command to export an encoded binary certificate to a file, for example: `certutil -ca.cert c:\Users\Administrator\Desktop\<MY_AD_cert>.cer` Where `<MY_AD_cert>` is a name you choose for the file. The file can be exported to any folder on the AD server
4. Copy the created certificate file to the CMS server using a utility such as WinSCP.
5. Log on to Linux as root on the CMS server.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.
6. Move to the directory to where you copied the certificate file in Step 4.
7. Run the following command on the CMS server to convert the binary certificate to a BASE-64 encoded certificate, a format required by the LDAP installation: `openssl x509 -inform DER -in <MY_AD_cert.cer> -out <MY_AD_cert.pem>`

   **Important:**

   Note the full path and file name of where you put the converted certificate. You must input the full path to the certificate file when installing the LDAP package with encryption.
8. After importing the certificate, you can install the LDAP feature package or update an existing installation of the LDAP feature package to use an encrypted connection.

# Installing the LDAP feature package on CMS

### Before you begin

Turn off CMS. Complete the following LDAP worksheet. This worksheet identifies the Active Directory server and encryption certificate information that you must enter when installing the LDAP package.

| Active Directory Server information | Example | Your Value |
|---|---|---|
| Enable optional encrypted LDAP connection (TLS/SSL) | yes, no | |

*Table continues…*

| Active Directory Server information | Example | Your Value |
|---|---|---|
| Path to certificate exported from LDAP server – must be provided when LDAP encryption=yes | /tmp/my_AD_cert.cer | |
| Windows Active Directory server IP Address or Fully Qualified Domain Name. An FQDN must be provided when LDAP encryption=yes | 10.20.30.40<br>or<br>ADServer.company.com | |
| Port number for the Active Directory server | 389 (default for TCP) 636 (default for TLS/SSL)<br>Or specific value from your AD server | |

## Procedure

1. Type `cmsadm` and press `Enter`. The system displays the following message:

```
Avaya(TM) Call Management System Administration Menu
Select a command from the list below.
1) acd_create Define a new ACD
2) acd_remove Remove all administration and data for an ACD
3) backup Filesystem backup
4) pkg_install Install a feature package
5) pkg_remove Remove a feature package
6) run_pkg Turn a feature package on or off
7) run_ids Turn Informix Database on or off
8) run_cms Turn Avaya CMS on or off
9) passwd_age Set password aging options
10) dbaccess Change Informix DB access permissions
11) config_pkg Configure a feature
Enter choice (1-11) or q to quit:
```

2. Type the number associated with the `pkg_install` option and press Enter. The system displays a message similar to the following, depending on which features you are licensed to install:

```
The CMS Features that can be installed are
1) forecasting
2) external call history
3) multi-tenancy
4) Dual IP
5) LDAP authentication
Enter choice (1-5) or q to quit:
```

3. Type the number that corresponds to the `LDAP Authentication` package and press Enter. The system displays the following message:

```
Do you want LDAP connections to be encrypted(TLS/SSL)? (y/n):
```

4. Do one of the following:
   - Type `Y` if you want to encrypt the LDAP connection. Continue with Step 5.
   - Type `N` if you do not want to encrypt the LDAP connection. Continue with Step 7.

5. The system displays the following message:

```
Enter the path to the certificate exported from LDAP server
(eg:/tmp/my_AD_cert.cer):
```

6. Type the location where you have imported the certificate and press `Enter`.The system displays the following message:

```
Enter the LDAP server IP Address or Fully Qualified Domain Name:
```

7. Type the IP address or FQDN of the LDAP server and press `Enter`.

   **Important:**

   When the LDAP connection is encrypted (TLS/SSL), you must enter an FQDN.

   The system displays the following message:

```
Enter the port number of the LDAP server (default: 636):
```

8. Enter the Windows server Active Directory port number and press `Enter`. The system displays the following message:

```
Enter the Bind Distinguished Name(eg: CN=Adm,OU=Users,DC=example,DC=com):
```

9. Type the Bind Distinguished Name and press `Enter`. For example, type: `CN=Administrator,CN=Users,DC=CPOD,DC=com`. The system displays the following message:

```
Enter the password for the Bind Distinguished Name:
```

10. Type the password for the Bind Distinguished Name and press `Enter`. The system displays the following message:

```
Retype the password for the Bind Distinguished Name:
```

11. Type the password for the Bind Distinguished Name again (it must be the same as the previous entry, or you will be required to re-enter) and press `Enter`. The system displays the following message:

```
Enter the Base Distinguished Name for CMS user authentication:
```

12. Type the Base Distinguished Name for CMS user authentication and press `Enter`. For example, `type: ou=CMSUsers,dc=CPOD,dc=com`. The system displays a message similar to the following example:

```
LDAP network connection is encrypted.
Secure(TLS) LDAP certificate path: /storage/my_ldap_cert.pem
LDAP server IP address or Fully Qualified Domain Name: host.example.com
Port Number for the LDAP server: 636
Bind Distinguished Name: CN=Administrator,CN=Users,DC=CPOD,DC=com
Bind Distinguished Password: *******
Base Distinguished Name: ou=CMSUsers,dc=CPOD,dc=com
Are the above inputs correct? (y/n, or q to quit): (default:n):
```

13. Do one of the following:

    - Type `Y` if the settings are correct.
    - Type `N` if the settings are not correct. The system will step you through each setting and allow you to change any of the settings.

14. The system verifies access to the Active Directory server and Based Distinguished Name, then displays the following message on successful installation of the package:

    ```
    LDAP authentication package installed.
    ```

15. If the installation failed, a message will display requesting input for the failed verification item(s). Input messages will continue until the inputs are successfully verified. To correct, verify the Active Directory Server values and accurate input.
16. Turn on CMS.

# Creating and migrating CMS users with LDAP authentication

### About this task

CMS offers a utility for bulk creation of LDAP-authenticated CMS users:`/cms/toolsbin/ldap_user_load`. With this tool, you can add the new users and modify existing users that use LDAP authentication. The ldap_user_load command adds LDAP users for specific CMS user login types: Normal User, Administrator, and Tenant User.

The command syntax is: `ldap_user_load [-n|-a|-t] cms_user_input_file`.

Where, `-n` is for Normal User

`-a` is for Administrator

`tn`t is for a Tenant User

`cms_user_input_file` is the name of the file that has the users you want to create.

You might want to run the command multiple times based on the login type (-n, -a, -t) to add unique groups of LDAP users The User Data screen allows the following login type updates for a modify action:

- Normal user to Administrator
- Administrator to Normal user

The following login type of updates are not allowed for a modify action:

- Normal user or Administrator to Tenant user
- Tenant user to Normal user or Administrator

When the Multi-Tenancy feature is installed, you should use the -n, -a, or -t options to add tenant users and not try to modify existing users.

**Important:**

The CMS user ID field supports 31 characters. However, for LDAP-authenticated users, you are limited to 20 characters. CMS user IDs up to 20 characters can be included in the cms_user_input_file.

### Before you begin

- Verify that you installed the LDAP feature.
- Turn on the CMS instance
- Determine which CMS users to add or modify with the LDAP authentication. The users must exist in the Base DN on the Active Directory server.

### Procedure

1. Create a file with a user name on each line. There is no limit to the number of users you can enter. The following is an example of creating the file `CmsUsersWithLDAPAuth` with users to add or modify existing users:

```
vi /tmp/CmsUsersWithLDAPAuth
ldap1
ldap2
:wq
```

2. Execute the LDAP authentication user load tool on the file you just created using the following command:`/cms/toolsbin/ldap_user_load /tmp/cmsUsersWithLDAPAuth`. The system displays output similar to the following example:

```
Processing user_id: ldap1
add for ldap1 successfully completed
Processing user_id: ldap2
modify for ldap2 successfully completed
LDAP user load completed Tue Apr 9 17:14:43 EDT 2019. 2 users processed.
1 ldap users added. 1 existing cms users where modified to ldap cms users.
0 user updates failed.
```

**Note:**

Users are not validated against the Active Directory server. If a user is added or modified that is not configured in the Base DN, subsequent CMS login attempts will fail since the user could not be authenticated. The file `/cms/install/ logdir/ldap_user_load.log` provides detailed information of the `/cms/ toolsbin/ldap_user_load` executions.The `/cms/install/cms_install/discarded_ldap_users` file provides the users that failed while running the ldap_user_load command. A failure message is also displayed. This includes specific failures attempted modify withlogin type changes.

To resolve these failures, review the `discarded_ldap_users` file to determine which users failed and the reason for failure. Correct the reason for failure for each user. Run the `ldap_user_load` command after you have fixed the errors found in the discarded_ldap_users. You can also use the discarded_ldap_users file as your new `cms_user_input_file` file.

3.

# Managing LDAP authenticated users in CMS

### About this task

When you install the LDAP authentication feature, the system presents a new LDAP Authentication field in the User Permissions: User Data screen to configure LDAP authentication. An LDAP authenticated user is a regular CMS user, except that the CMS login is authenticated with the password configured on the LDAP directory server.

### Before you begin

Install the LDAP feature package if not already installed. Turn on the CMS

### Procedure

1. Log in to the CMS as a user that is an administrator.
2. Go to **User Permission** > **User Data**.
3. View, add, modify users as needed.

**Note:**

Users that are added or modified for LDAP Authentication but are not configured on the Active Directory server will be successfully added. The user will not be able to log on to CMS since it cannot be authenticated.

# Adding a secondary IP address to an ACD

### About this task

After the Dual IP feature is installed, you can administer a secondary IP address on an existing ACD or a new ACD.

### Before you begin

Turn off CMS.

### Procedure

1. Log on as root.

**Important:**

You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

2. Enter: `cmssvc`.
3. Select the **swsetup** option.
4. Select the ACD you want to change.
5. At the secondary switch prompts, add the required information.

6. Review the data you entered. For example,

```
Switch name: abc
Switch model: Communication Mgr 8.x
Local port: 1
Remote port: 1
Link: TCP/IP cmsvm10 5001
Secondary link: TCP/IP cmsvm10 5002
```

7. If the data is correct, enter `Y`..
8. Turn on CMS

## To add a secondary IP address while adding a new ACD

### Procedure

1. Log on as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

2. Do one of the following steps to add a new ACD: To set up the initial system configuration, add all ACDs as shown in Configuring the standard CMS options. At the secondary switch prompts, add the required information.To create a new ACD on an existing system, add a new ACD is shown in Using `acd_create`. At the secondary switch prompts, add the required information.
3. Review the data you entered. For example:

```
Switch name: abc
Switch model: Communication Mgr 8.x
Local port: 1
Remote port: 1
Link: TCP/IP cmsvm10 5001
Secondary link: TCP/IP cmsvm10 5002
```

4. If the data is correct, enter `Y`.
5. Turn on CMS.

# Activating the CMS Supervisor Web Client software

The CMS Supervisor Web Client software is installed on the same server as the CMS software. The Web Client is browser-based and allows customers to access CMS administration and reports without install client software on your computer.

For more information, see *Avaya Call Management System Overview and Specification* and *Avaya Call Management System Overview and Specification*

# Starting the Web Client software

## Procedure

1. Log in to the CMS server with root privileges.

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

2. Run the `cmsweb start` command.

3. Run the `rpm -qa cmsweb` to ensure that the correct version of the Web Client software is installed.

# Generating a certificate for the Web Client server

## About this task

Generate a security certificate to encrypt communications between your browser and the CMS Supervisor web server. After generating a key, create a Certificate Signing Request (CSR) and then you use that to get a CA certificate.

## Procedure

1. Log in to the CMS server with root privileges.

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

2. Run the `mkdir /opt/cmsweb/cert/custom` command to create a directory for the new Web Client certificate.

   If you navigate away from the directory, you can run `cd /opt/cmsweb/cert/custom` to switch back to it.

3. Run the following command to generate a new key and keystore:

   ```
   keytool -genkey -alias cmsweb -keyalg RSA -keysize 4096 -keystore cmsweb.p12
   -dname "CN=[fqdn],OU=XX,O=XX,L=XX,ST=XX,C=XX" -ext "SAN=IP:[ip],DNS:[fqdn]"
   ```

   Replace XX with the appropriate certificate details. Replace [ip] and [fqdn] with the CMS web server IP address and FQDN.

   For the password, enter `cmsweb`.

4. Run the following command to generate a certificate request:

   ```
   keytool -certreq -keyalg RSA -alias cmsweb -file cmsweb.csr -keystore cmsweb.p12
   ```

   Enter `cmsweb` as the password.

5. Use the CSR certificate request in the file `cmsweb.csr` to get a certificate from the CA of your choice.

# Installing the root certificate for the Web Client software

## About this task

Sometimes the CA also issues an intermediate CA certificate. If the CA issues an intermediate certificate, import the intermediate CA certificate using the steps in this procedure. If you do not have an intermediate certificate, skip those optional steps.

## Procedure

1. Copy and paste the CA root certificate into a file, for example, `root.crt`.
2. Use the following command to import the root certificate:

   ```
   keytool -import -alias root -keystore cmsweb.p12- trustcacerts
   -file root.crt
   ```

3. For the password, enter `cmsweb`.

   **Note:**

   Do Steps 4–6 if the intermediate certificates are published and required by the CA.

4. Copy and paste the intermediate certificate into a file, for example, `intermediate.cert.`
5. Use the following command to import the certificate:

   ```
   keytool -import -alias intermediate -keystore cmsweb.p12
   -trustcacerts -file intermediate.cert
   ```

6. For the password, enter `cmsweb1`.
7. Copy and paste the new certificate into a file, for example, `cmsweb.cert`.
8. Use the following command to import the certificate:

   ```
   keytool -import -alias cmsweb -keystore cmsweb.p12 -trustcacerts
   -file cmsweb.cert
   ```

9. For the password, enter `cmsweb`.
10. Use the following command to stop the Web Client software:

    ```
    cmsweb stop
    ```

11. Copy the keystore in the correct location, for example

    ```
    cp /opt/cmsweb/cert/custom/cmsweb.p12 /opt/cmsweb/cert
    ```

12. Use the following command to start the Web Client software:

    ```
    cmsweb start
    ```

# Configuring EASG

## Before you begin

Use the cmssvc command to enable or disable EASG. You can enable or disable EASG without affecting CMS operations. You can also view the EASG certificate.

### Procedure

1. Log on to the CMS server as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

2. At the prompt, type `cmssvc` and press `Enter`.The system displays the following **Avaya Call Management System Services** Menu:

```
Avaya(TM) Call Management System Services Menu
Select a command from the list below.
1) auth_display Display feature authorizations
2) weblm_set Set up the connection to the WebLM
3) run_ids Turn Informix Database on or off
4) run_cms Turn Avaya CMS on or off
5) setup Set up the initial configuration
6) swinfo Display switch information
7) swsetup Change switch information
8) uninstall Remove the CMS rpm from the machine
9) patch_rmv Backout an installed CMS patch
10) back_all Backout all installed CMS patches from machine
11) security Administer CMS security features
Enter choice (1-11) or q to quit: 1
```

3. Type `11` and press `Enter`. The system displays the following output:

```
Select one of the following:
1) FIPS 140-2 mode
2) Firewall
3) Enhanced Access Security Gateway (EASG)
4) Disk encryption
Enter choice (1-4) or q to quit:
```

4. Type `3` and press `Enter`. The system displays the following output:

```
Select one of the following
1) Disable EASG
2) Enable EASG
3) Display EASG Certificate
Enter choice (1-3) or q to quit:
```

5. Type the appropriate number and press `enter`.

# Setting up the Alarm Origination Manager

Use this section to set up the Alarm Origination Manager (AOM) on the CMS server. You can use the AOM feature to enable alarming to Avaya and this capability is available only for CMS servers with a current maintenance agreement in effect. You can optionally use AOM to send SNMP alarms to customer provided Network Management Systems (NMS). You can enable SNMP alarms to a customer provided NMS even if a current Avaya maintenance agreement is not in effect.

## Prerequisites

Before you set up AOM, do the following tasks: Obtain an Alarm ID number and Sold To Functional Location (FL) number. You can obtain an Alarm ID by registering the CMS server. You can register a CMS server using the Avaya Global Registration Tool (GRT) tool at https://support.avaya.com/grt.

If you cannot register the system using the GRT tool, call 1800-242-2121, extension 15265, for assistance. If the system does not have an Avaya maintenance agreement in effect and you are going to configure optional SNMP alarming in a customer NMS, accept the default values that are pre-populated.

**Note:**

During AOM configuration, use the Alarm ID referred to here as the Alarm ID and use the Sold To Functional Location (FL) number as the Customer ID. You must login as a root.

**Important:**

You cannot directly log on as root from a remote connection. You must log onusing an administered CMS user ID, then use `su - root` to log on with root privileges

# Setting up AOM configuration for SNMP alarming

The aom_tool is used to configure AOM.

**Important:**

CMS supports only SNMP v3 in this release.

# Configuring AOM

There are multiple phases to completing the AOM configuration. You must configure an Alarm ID, and you must configure a Customer ID if SNMP alarming is used. If you want to use SNMP, you must configure an SNMP user. Finally, you must configure an Alarm Destination.

**Note:**

Configuring an Alarm destination includes configuring Alarm ID and Customer ID. Customer ID is only configured if SNMP alarming is used.

# Configuring an Alarm Destination

## Procedure

1. Start the AOM tool by running the following command:

```
/cms/aom/bin/aom_tool
```

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the Configure the Alarm Destination option, and press `Enter`.

```
Welcome to Avaya CMS Alarm Origination main menu.
1) SNMP/SAL
2) Socket/SAL
q) Quit
Enter choice (1-2, q):
```

**Note:**

Avaya recommends using SNMP/SAL for alarming.

3. Enter the number associated with the SNMP/SAL option, and press Enter. The system displays a list of SNMP configuration options:

```
Do you want to
1) Add an SNMP Connection
2) Delete an SNMP Connection
3) Modify an SNMP Connection
4) Add an SNMP User
5) Delete an SNMP User
6) Modify an SNMP User
7) Clear SNMP Alarms
q) Quit
Enter choice (1-7, q):
```

4. Enter the number associated with the **Add an SNMP connection** option, and press `Enter`. The system displays the **Adding an SNMP connection** option followed by an input prompt for destination type:

```
Adding an SNMP connection
Select a destination type:
1) SAL
2) NMS
Enter choice (1-2):
```

5. Enter the number associated with SAL or NMS, and press `Enter`.The system displays the input prompt for the destination IP address:

```
What is the destination IP address?
```

6. Enter the destination IP address, for example, 192.168.123.256, and press `Enter`. The system displays the input prompt for the port number:

```
What is the destination port number?
```

7. Enter the destination port number, for example, 162, and press `Enter`. The system displays the input prompt for the SNMP user:

```
Select an SNMP user:
1) cmssnmp
Enter choice (1-1):
```

8. The system displays a list of defined users. Select an SNMP user, and press `Enter`. The system displays the input prompt for Alarm ID along with the default Alarm ID value:

```
What is the Alarm ID (10 digit alarm ID)? (default:3000004043)
```

9. Enter the Alarm ID or accept the default value, and press `Enter`. The system displays the input prompt for Customer ID along with the default Customer ID:

```
What is the Customer ID (10 digit customer code)? (default:0004558769)
```

10. Enter the Customer ID value or accept the default value, and press `Enter`.The system displays the input prompt for Customer Name along with the default CustomerName value:

```
What is the Customer Name? (default:Avaya)
```

11. Enter the Customer Name or accept the default value, and press `Enter`. The system displays the input prompt for running a test alarm:

```
Run a test alarm when done?(y/n)
```

12. Enter `Y` or `N`, and press `Enter`. The system displays the following messages:

```
You have selected to configure AOM using SNMP.
Add an SNMP Connection
Destination Type: SAL
Destination IP: 198.1.1.2
Destination port: 162
Notification Type: inform
User Name: salcmsuser
Alarm ID: 3000004043
Customer ID: 0004558769
Customer NAME: Avaya
A test alarm will be sent at the end.
Press [Enter] to continue or [q] to quit
```

**Note:**

The SAL SNMP option requires a Notification Type of inform and notify in the `dest.cfg` file.

13. Press `Enter`. The system displays the following messages:

```
Configuring dest.cfg
[started]
done
reset AOM
[started]
done
Clearing all current alarms.
[started]
done
Sending test alarm.
[started]
done
done
Do you want to
```

```
1) Add an SNMP Connection
2) Delete an SNMP Connection
3) Modify an SNMP Connection
4) Add an SNMP User
5) Delete an SNMP User
6) Modify an SNMP User
7) Clear SNMP Alarms
q) Quit
Enter choice (1-7, q): q
```

14. Enter `Q` to quit, and press `Enter`. The system displays the following message:

```
Quitting…
```

# Configuring an SNMP User

## Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`.The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the Configure the Alarm Destination option, and press `Enter`. The system displays the Welcome to Avaya CMS Alarm Origination main menu options:

```
Welcome to Avaya CMS Alarm Origination main menu.
1) SNMP/SAL
2) Socket/SAL
q) Quit
Enter choice (1-2, q):
```

**Note:**

Avaya recommends using SNMP/SAL for alarming.

3. Enter the number associated with the SNMP/SAL option, and press `Enter`. The system displays the list of SNMP configuration options:

```
Do you want to
1) Add an SNMP Connection
2) Delete an SNMP Connection
3) Modify an SNMP Connection
4) Add an SNMP User
5) Delete an SNMP User
6) Modify an SNMP User
7) Clear SNMP Alarms
q) Quit
Enter choice (1-7, q):
```

4. Enter the number associated with the Add an SNMP User option, and press `Enter` The system displays the input prompt for SNMP user name:

```
Adding an SNMP user
What is the SNMP user name?
```

5. Enter the SNMP user name, and press `Enter`.The system displays the Select the SNMP version option:

```
Select the SNMP version:
1) v3
Enter choice (1-1):
```

6. Enter the number associated with the v3 option, and press `Enter`. The system displays the Select the access level option:

```
Select the access level:
1) rouser: Read Only
2) rwuser: Read/Write
Enter choice (1-2):
```

7. Enter the number associated with the level of access to assign to the user, and press `Enter`.The system displays the Select the security level option based on the FIPS status:

   If the FIPS mode is off:

```
Select the security level:
1) noAuthNoPriv: Unauthenticated/Unencrypted (not allowed in FIPS mode)
2) authNoPriv: Authenticated/Unencrypted (not allowed in FIPS mode)
3) authPriv: Authenticated/Encrypted
Enter choice (1-3):
```

   If the FIPS mode is on:

```
Select the security level:
3) authPriv: Authenticated/Encrypted
Enter choice (1-1):
```

8. Enter the number associated with the level of security to assign to the user, and press `Enter`. The system displays the Select the authentication protocol option based on the FIPS status:

   If the FIPS mode is off:

```
Select the authentication protocol:
1) MD5 ( not allowed in FIPS mode)
2) SHA
Enter choice (1-2):
```

   If the FIPS mode is on:

```
Select the authentication protocol:
1) SHA
Enter choice (1-1):
```

9. Enter the number associated with the authentication protocol to assign to the user, and press `Enter`.

**Note:**

Authentication utilizes the defined authentication password to sign the messages that are sent during authentication. The encryption protocol for this can be either MD5 or SHA.

The system displays the authentication password prompt:

```
Enter authentication password (min 8 chars):
```

10. Enter the authentication password to assign to the user, and press `Enter`. The system displays the Select the encryption protocol option:

```
Select the encryption protocol:
1) AES
2) DES
Enter choice (1-2):
```

11. Enter the number associated with the encryption protocol to assign to the user, and press `Enter`.

**Note:**

Authentication utilizes the defined encryption password to encrypt the data portion of the SNMP messages. The encryption protocol for this may be either AES or DES.

The system displays the encryption password prompt:

```
Enter encryption password (min 8 chars):
```

12. Enter the encryption password to assign to the user, and press `Enter`. The system displays information about the choices entered:

```
CMS was last rebooted 11 day(s) ago.
You have selected to configure AOM using SNMP.
Add an SNMP User
User Name: TestSNMP
SNMP version: v3
SNMP Access Level: rouser
SNMP Security Level: authPriv
SNMP authentication protocol: MD5
SNMP authentication password: ******
SNMP encryption protocol: AES
SNMP encryption password: ******
Press [Enter] to continue or [q] to quit
```

13. Press `Enter` to save the choices displayed, or press `Q` to quit.

14. If you press `Enter`, the system saves the choices and displays the following messages:

```
Configuring /cms/aom/data/admin/user.cfg
[started]
Done
Do you want to
1) Add an SNMP Connection
2) Delete an SNMP Connection
3) Modify an SNMP Connection
4) Add an SNMP User
5) Delete an SNMP User
6) Modify an SNMP User
7) Clear SNMP Alarms
```

```
q) Quit
Enter choice (1-7, q):
```

- To add another user, repeat Steps 3-13.
- To modify a user, enter the number associated with the Modify an SNMP User, and press `Enter`. Make any desired changes to the configuration of the user.
- Press `Q` to quit.

# Configuring an Alarm ID

## Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`. The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the **Set Alarm ID** option, and press `Enter`. The system displays the Alarm ID prompt:

```
What is the Alarm ID (10 digit alarm ID)? (default:3000004043)
```

Enter the Alarm ID that was obtained from either the Avaya GRT or Automatic Registration Tool (ART) tool, and press `Enter`.

**Note:**

The default Alarm ID is normally the last value entered. CMS servers have a pre-defined default value that must be changed if the customer has an Avaya maintenance agreement.

After you configure the Alarm ID, the system displays the following messages, and the tool returns to the command line prompt:

```
reset AOM
[started]
Done
#
```

# Configuring a Customer ID

## Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`.The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the Customer ID option, and press `Enter`.The system displays the Customer ID prompt:

```
What is the Customer ID (10 digit customer code)? (default:0004558769)
```

3. Enter the Customer ID value, and press `Enter`.

   **Note:**

   The default Customer ID is normally the last value entered. CMS servers have a pre-defined default value that must be changed if the customer has an Avaya maintenance agreement.

   The system displays the Customer Name prompt:

```
What is the Customer Name? (default:)
```

4. Enter the Customer Name, and press `Enter`. After you have configured the Customer name, the system displays the following messages, and the tool returns to the command line prompt:

```
reset AOM
[started]
Done
#
```

# Sending an AOM Test Alarm

## Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`.The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the **Send a Test Alarm** option, and press `Enter`. The system clears the current alarms and then sends the test alarm. The system displays the following messages, and the tool returns to the command line prompt.

```
Clearing all current alarms.
[started]
done
Sending test alarm.
[started]
done
#
```

# Clearing SNMP Alarms

## Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`.The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the Configure the Alarm Destination option, and press `Enter`. The system displays the **Welcome to Avaya CMS Alarm Origination** main menu options:

```
Welcome to Avaya CMS Alarm Origination main menu.
1) SNMP/SAL
2) Socket/SAL
q) Quit
Enter choice (1-2, q):
```

**Note:**

Avaya recommends using SNMP/SAL for alarming.

3. Enter the number associated with the SNMP/SAL option, and press `Enter`. The system displays the list of SNMP configuration options:

```
Do you want to
1) Add an SNMP Connection
2) Delete an SNMP Connection
3) Modify an SNMP Connection
4) Add an SNMP User
5) Delete an SNMP User
6) Modify an SNMP User
7) Clear SNMP Alarms
q) Quit
Enter choice (1-7, q): 7
```

4. Enter the number associated with the Clear SNMP Alarms option, and press `Enter`.

5. The system displays active alarms. To close an open alarm, press `Y` at the prompt.

## CMS SNMP alarm information

| Alarm type | Alarm name | SNMP object identifier | Description |
|---|---|---|---|
| Test Alarm | TEST_ALARM | 1.3.6.1.4.1.6889.2.72.0.1 This | This Test alarm is generated to verify that CMS alarming is functional. Since this is a test alarm, this alarm does not cause a new alarm ticket to be created with Avaya. |
| Test Alarm Clear | TEST_ALARM_CLR | 1.3.6.1.4.1.6889.2.72.0.2 | This Test alarm clear is generated to verify that CMS alarming is functional. Since this is a test alarm clear, this alarm does not close all alarm tickets with Avaya. |
| Expert System Alarm | ES_ALARM | 1.3.6.1.4.1.6889.2.72.0.3 | Avaya Expert System alarm. |
| Expert System Alarm Clear | ES_ALARM_CLR | 1.3.6.1.4.1.6889.2.72.0.4 | Avaya Expert System alarm clear. |
| ACD Link Alarm | ACDLINK[1-8] | 1.3.6.1.4.1.6889.2.72.0.5 | This ACD Link Alarm is generated if any CMS ACD link experiences trouble. |
| ACD Link Alarm Clear | ACDLINK[1-8]_CLR | .1.3.6.1.4.1.6889.2.72.0.6 | This ACD Link Alarm Clear is generated when an existing ACD Link alarm is cleared. |
| Archiving Alarm | [H]*ARCH | .1.3.6.1.4.1.6889.2.72.0.7 | This Archiving Alarm is generated when the CMS interval, daily, weekly, or monthly data archiver experiences trouble. |
| Archiving Alarm Clear | [H]*ARCH_CLR | 1.3.6.1.4.1.6889.2.72.0.8 | This Archiving Alarm Clear is generated when an existing data archiver alarm is cleared. |
| Disk Error | DISK _ERR | 1.3.6.1.4.1.6889.2.72.0.9 | This disk error alarm is generated when a disk failure occurs. |

*Table continues…*

| Alarm type | Alarm name | SNMP object identifier | Description |
|---|---|---|---|
| Disk Error Clear | DISK_ERR_CLR | 1.3.6.1.4.1.6889.2.72.0.10 | This disk error clear alarm is generated when an existing DISK_ERR alarm is cleared. |
| ECH Warning Alarm | ECH_WARNING | 1.3.6.1.4.1.6889.2.72.0.11 | This ECH Warning Alarm is generated when External Call History experiences a warning. |
| ECH Warning Alarm Clear | ECH_WARNING_CLR | 1.3.6.1.4.1.6889.2.72.0.12 | This ECH Warning Alarm Clear is generated when an existing ECH. Warning alarm is cleared |
| ECH Failure Alarm | ECH_FAILURE | 1.3.6.1.4.1.6889.2.72.0.13 | This ECH Failure Alarm is generated when External Call History experiences a failure. |
| ECH Failure Alarm Clear | ECH_FAILURE_CLR | 1.3.6.1.4.1.6889.2.72.0.14 | This ECH Failure Alarm Clear is generated when an existing ECH Failure alarm is cleared. |
| Surviving Alarm | SURVIVING | .1.3.6.1.4.1.6889.2.72.0.15 | This Surviving Alarm is generated when a survivable CMS in standby mode becomes active. |
| Surviving Alarm Clear | SURVIVING_CLR | 1.3.6.1.4.1.6889.2.72.0.16 | This Surviving Alarm Clear is generated when an existing Surviving Alarm is cleared. |
| Disk Warning | DISK_WRN | .1.3.6.1.4.1.6889.2.72.0.17 This | This disk warning alarm is generated when a disk warning occurs. A disk warning indicates a disk failure condition that can exist in the near future. |
| Disk Warning Clear | DISK_WRN_CLR | 1.3.6.1.4.1.6889.2.72.0.18 | This disk warning clear alarm is generated when an existing DISK_WRN alarm is cleared. |
| Battery Error | BATTERY_ERR | 1.3.6.1.4.1.6889.2.72.0.19 | This battery error alarm is generated when a RAID battery failure occurs. |

*Table continues…*

| Alarm type | Alarm name | SNMP object identifier | Description |
|---|---|---|---|
| Battery<br>Error Clear | BATTERY_ERR_CLR | 1.3.6.1.4.1.6889.2.72.0.20 | This battery error clear alarm is generated when an existing BATTERY_ERR alarm is cleared. |
| Battery<br>warning | BATTERY_WRN | 1.3.6.1.4.1.6889.2.72.0.21 | This battery warning alarm is generated when a RAID battery warning occurs. A battery warning indicates a RAID battery failure condition that can exist in the near future. |
| Battery<br>Warning<br>Clear | BATTERY_WRN_CLR | .1.3.6.1.4.1.6889.2.72.0.22 | This battery warning clear alarm is generated when an existing BATTERY_WRN alarm is cleared. |
| RAID Error | RAID_ERR | .1.3.6.1.4.1.6889.2.72.0.23 | This RAID error alarm is generated when a RAID enclosure failure occurs. |
| RAID Error Clear | RAID_ERR_CLR | 1.3.6.1.4.1.6889.2.72.0.24 | This RAID error clear alarm is generated when an existing RAID_ERR alarm is cleared. |
| RAID Warning | RAID_WRN | 1.3.6.1.4.1.6889.2.72.0.25 | This RAID warning alarm is generated when a RAID enclosure warning occurs. A RAID warning indicates a RAID enclosure failure condition that can exist soon. |
| RAID Warning Clear | RAID_WRN_CLR | 1.3.6.1.4.1.6889.2.72.0.26 | This RAID warning clear alarm is generated when an existing RAID_WRN alarm is cleared. |
| Backup<br>Warning | BACKUP_WRN | 1.3.6.1.4.1.6889.2.72.0.27 | This backup warning alarm is generated when a CMS maintenance backup warning occurs. A backup warning indicates that a CMS maintenance backup was not successful. |

*Table continues…*

| Alarm type | Alarm name | SNMP object identifier | Description |
|---|---|---|---|
| Backup Warning Clear | BACKUP_WRN_CLR | .1.3.6.1.4.1.6889.2.72.0.28 | This backup warning clear alarm is generated when an existing BACKUP_WRN alarm is cleared |
| Elog Warning Alarm | ELOG_WRN | 1.3.6.1.4.1.6889.2.72.0.29 | Warning that the CMS error logging process may be overloaded. |
| ElogWarning Alarm Clear | ELOG_WRN_CLR | 1.3.6.1.4.1.6889.2.72.0.30 | CMS ELOG_WRN clear. |
| ACD Secondary Link Up | ACDSECUP[1-8] | 1.3.6.1.4.1.6889.2.72.0.31 | The secondary ACD IP address is being used. |
| ACD Secondary Link Up Clear | ACDSECUP[1-8]_CLR | 1.3.6.1.4.1.6889.2.72.0.32 | The Clear is generated when the ACD Secondary Link Up Alarm is cleared. |
| Disk Full Warning | DISKFULLINF | .1.3.6.1.4.1.6889.2.72.0.33 | This Disk Full Alarm is generated when the disks are 95% full. |
| Disk Full Warning Clear | DISKFULLINF_CLR | 1.3.6.1.4.1.6889.2.72.0.34 | This Disk Full Warning Clear is generated when the Disk Full Warning is cleared. |
| Disk Full Alarm | DISKFULLWRN | 1.3.6.1.4.1.6889.2.72.0.35 | This Disk Full Alarm is generated when the disks are 95% full. |
| Disk Full Alarm | DISKFULLWRN_CLR | 1.3.6.1.4.1.6889.2.72.0.36 | The Disk Full Alarm is cleared. |
| Firewall Warning Alarm | FIREWALLWRN | 1.3.6.1.4.1.6889.2.72.0.37 | This firewall warning is generated when the firewall is disabled |
| Firewall Warning Alarm Clear | FIREWALLWRN_CLR | 1.3.6.1.4.1.6889.2.72.0.38 | The firewall warning is cleared. |
| FIPS Warning Alarm | FIPS_WRN | .1.3.6.1.4.1.6889.2.72.0.39 | This FIPS warning is generated when FIPS is disabled. |
| FIPS Warning Alarm Clear | FIPS_WRN_CLR | 1.3.6.1.4.1.6889.2.72.0.40 | The FIPS Warning Alarm is cleared |
| WebLM Warning Alarm | LIC_ERR | 1.3.6.1.4.1.6889.2.72.0.41 | This License error is generated when CMS is in license error mode. |
| WebLM Warning Alarm Clear | LIC_ERR_CLR | 1.3.6.1.4.1.6889.2.72.0.42 | The license error mode is cleared. |

*Table continues…*

| Alarm type | Alarm name | SNMP object identifier | Description |
|---|---|---|---|
| WebLM Warning Alarm | LIC_RESTRICTED | 1.3.6.1.4.1.6889.2.72.0.43 | This License Restricted is generated when CMS is in license restricted mode. |
| WebLM Warning Alarm Clear | LIC_RESTRICTED_CLR | 1.3.6.1.4.1.6889.2.72.0.44 | The license restricted mode is cleared. |
| Web Client Warning Alarm | WEBCRT_WRN | 1.3.6.1.4.1.6889.2.72.0.45 | This Web Client certificate warning alarm is generated when the Web Client certificate is about to expire. |
| Web Client Warning Alarm Clear | WEBCRT_WRN_CLR | 1.3.6.1.4.1.6889.2.72.0.46 | The Web Client certificate warning alarm is cleared. |
| Web Client Error Alarm | WEBCRT_ERR | 1.3.6.1.4.1.6889.2.72.0.47 | This Web Client certificate error alarm is generated when the Web Client certificate has expired. |
| Web Client Error Alarm Clear | WEBCRT_ERR_CLR | 1.3.6.1.4.1.6889.2.72.0.48 | The Web Client certificate expired error alarm is cleared. |
| EASG Warning Alarm | EASGCRT365_WRN | 1.3.6.1.4.1.6889.2.72.0.49 | This EASG certificate warning alarm is generated when the EASG certificate is expiring within 365 days. |
| EASG Warning Alarm Cleared | EASGCRT365_WRN_CLR | 1.3.6.1.4.1.6889.2.72.0.50 | The EASG certificate 365 day warning alarm is cleared. |
| EASG Warning Alarm | EASGCRT180_WRN | 1.3.6.1.4.1.6889.2.72.0.51 | This EASG certificate warning alarm is generated when the EASG certificate is expiring within 180 days. |
| EASG Warning Alarm Cleared | EASGCRT180_WRN_CLR | 1.3.6.1.4.1.6889.2.72.0.52 | The EASG certificate 180 day warning alarm is cleared. |
| EASG Warning Alarm | EASGCRT30_WRN | 1.3.6.1.4.1.6889.2.72.0.53 | This EASG certificate warning alarm is generated when the EASG certificate is expiring within 30 days. |

*Table continues…*

| Alarm type | Alarm name | SNMP object identifier | Description |
|---|---|---|---|
| EASG Warning Alarm Cleared | EASGCRT30_WRN_CLR | 1.3.6.1.4.1.6889.2.72.0.54 | The EASG certificate 30 day warning alarm is cleared. |
| EASG Error Alarm | EASGCRT30_ERR | 1.3.6.1.4.1.6889.2.72.0.55 | This EASG certificate error alarm is generated when the EASG certificate has expired. |
| EASG Error Alarm Cleared | EASGCRT30_ERR_CLR | 1.3.6.1.4.1.6889.2.72.0.56 | The EASG certificate expired error alarm is cleared |

# Locating the CMS-MIB.txt file

You can also download `CMS-MIB.txt` from http://support.avaya.com and install this file with NMS.

# Configuring an Alarm Destination

### Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`. The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the Configure the Alarm Destination option, and press `Enter`. The system displays the following message:

```
Welcome to Avaya CMS Alarm Origination main menu.
1) SNMP/SAL
2) Socket/SAL
q) Quit
Enter choice (1-2, q):
```

3. Enter the number associated with the Socket/SAL option, and press `Enter`.

**Note:**

If the system has been previously configured with an alarming method, the system can prompt for the removal of the configuration.

The system displays the input prompt for the **SAL IP** address:

```
What is the SAL ip address?
```

4. Enter the **SAL IP** address, and press `Enter`.

   **Important:**

   Do not use any leading zeros in the IP address as this can lead the system to interpret the numbers in the address as octal.

   The system displays the input prompt for the SAL network port and the default network port value:

   ```
   What is the SAL network port? (default:5108)
   ```

5. Enter the **SAL network port** value or accept the default value, and press `Enter`. The system displays the input prompt for the **Alarm ID** and the default **Alarm ID:**

   ```
   What is the Alarm ID (10 digit product code)?
   ```

6. Enter the **Alarm ID** or accept the default value, and press `Enter`. The system displays the input prompt for running a test alarm:

   ```
   Run a test alarm when done?(y/n)
   ```

7. Enter `Y` or `N`, and press `Enter`.

   The system displays the following messages:

   ```
   CMS was last rebooted 1 day(s) ago.
   You have selected to configure AOM using SAL via Socket/Virtual NIU.
   Removing existing socket configuration
   SAL IP Address:
   SAL network port number: 5108
   Alarm ID: 3000004043
   A test alarm will be sent at the end.
   Press [Enter] to continue or [q] to quit
   ```

8. Press `Enter`.

   The system displays the following messages, and the tool returns to the command line prompt:

   ```
   Configuring dest.cfg
   [started]
   done
   reset AOM
   [started]
   done
   Clearing all current alarms.
   [started]
   done
   Sending test alarm.
   [started]
   done
   done#
   ```

# Configuring an Alarm ID

## Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`.The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the **Set Alarm ID** option, and press `Enter`. The system displays the Alarm ID prompt:

```
What is the Alarm ID (10 digit alarm ID)? (default:3000004043)
```

3. Enter the **Alarm ID** that was obtained from either the Avaya GRT or Automatic Registration Tool (ART) tool, and press `Enter`.

   **Note:**

   The default Alarm ID is normally the last value entered. CMS servers have a pre-defined default value that must be changed if the customer has an Avaya maintenance agreement.

   After you configure the Alarm ID, the system displays the following messages, and the tool returns to the command line prompt:

```
reset AOM
[started]
Done
#
```

# Sending an AOM Test Alarm

## Procedure

1. Start the AOM tool by running the following command: `/cms/aom/bin/aom_tool`.The system displays the following messages:

```
Welcome to Avaya CMS Alarm Configuration Main Menu.
1) Set Alarm ID
2) Set Customer ID
3) Configure Alarm Destination
4) Send a Test Alarm
q) Quit
Enter choice (1-4, q):
```

2. Enter the number associated with the **Send a Test Alarm** option, and press `Enter`

The system clears the current alarms and then sends the test alarm. The system displays the following messages, and the tool returns to the command line prompt.

```
Clearing all current alarms.
[started]
done
Sending test alarm.
[started]
done
#
```

# Setting the Informix configuration parameters for CMS

The IDS configuration parameters for CMS are automatically optimized for system performance during the installation of Informix.

# Chapter 5: Maintaining CMS

## Using the CMSADM menu

This section describes how to use the options in the **Avaya Call Management System Administration Menu** (CMSADM menu). The CMSADM menu is intended for use by the CMS administrator

**Related links**


CMSADM menu functions on page 60
Accessing the CMSADM menu on page 61
Defining a new ACD (acd_create) on page 61
Removing an ACD (acd_remove) on page 62
Backing up the file system (backup) on page 63
Installing feature packages (pkg_install) on page 64
Removing feature packages (pkg_remove) on page 64
Turning a feature package on/off (run_pkg) on page 65
Turning IDS on/off (run_ids) on page 66
Turning CMS on/off (run_cms) on page 66
Switching password aging on/off (passwd_age) on page 67
Controlling ODBC/JDBC database access (dbaccess) on page 68
Configuring a feature package (config_pkg) on page 70


## CMSADM menu functions

The following list shows the tasks that the CMS administrator can do from the CMSADM menu:

- Define a new Automatic Call Distribution (ACD).
- Remove an ACD.
- Back up the file systems to tape.
- Install or remove a feature package.
- Turn a feature package on or off.
- Turn the IDS software on or off.
- Turn the CMS software on or off.
- Turn password aging on or off.
- Change Informix DB access permissions.

- Change configuration for an installed feature package.

**Related links**

Using the CMSADM menu on page 60

# Accessing the CMSADM menu

## About this task

You can use this process to display the CMS administration menu.

- The options displayed in the menu vary depending on the version of CMS.
- You cannot access **cmsadm** or **cmssvc** commands whilst another user or process is running a **cmssvc** setup command. When this occurs, CMS displays a **Please try later, setup is active** error message.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.

```
Avaya(TM) Call Management System Administration Menu
Select a command from the list below.
1) acd_create Define a new ACD
2) acd_remove Remove all administration and data for an ACD
3) backup Filesystem backup
4) pkg_install Install a feature package
5) pkg_remove Remove a feature package
6) run_pkg Turn a feature package on or off
7) run_ids Turn Informix Database on or off
8) run_cms Turn Avaya CMS on or off
9) passwd_age Set password aging options
10) dbaccess Change Informix DB access permissions
11) config_pkg Configure a feature
Enter choice (1-11) or q to quit:
```

**Related links**

Using the CMSADM menu on page 60

# Defining a new ACD (acd_create)

## About this task

You can use this process to add a new ACD.

When you add an ACD, the system automatically grants permission to the ACD for administrator and normal users, but not to tenant users. You must manually give permission to the ACD for tenant users.

## Before you begin

1. You must purchase and authorize the ACD before you add it to CMS.
2. If you want to administer a secondary hostname or IP address, you must install the Dual IP feature package before creating the ACD.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Turn off the CMS software:
   a. Select `run_cms`.
   b. Select Enter the number to turn off the CMS software.
4. Enter the number associated with the **acd_create** option. CMS selects the next available ACD for creation. For example, if two ACDs are already active, CMS selects ACD 3.
5. At the prompts, enter the information for the new ACD:

- Switch name
- Switch model (release)
- Local port assigned to the switch
- Remote port assigned to the switch
- The hostname or IP address and TCP port
- The optional secondary host name or IP address and TCP port if the Dual IP feature is installed
- Number of splits/skills
- Total split/skill members, summed over all splits/skills
- Start and stop times of all shifts
- Number of trunk groups
- Number of trunks
- Number of unmeasured (trunk) facilities
- Number of call work codes

6. Restart the CMS software:
   a. Enter the number associated with the `run_cms` option.
   b. Enter the option to turn on the CMS software.

**Related links**

Using the CMSADM menu on page 60

# Removing an ACD (acd_remove)

### About this task

You can use this process to remove an ACD.

When you remove an ACD, the system reassigns all users from the removed ACD to the master ACD. Tenant users assigned to only the removed ACD will not be able to access CMS until they are reassigned to a new ACD.

**Important:**

- You cannot remove the master ACD. If you want to remove an ACD that is currently designated as the master ACD, you must designate another ACD as the master ACD.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Turn off the CMS software:
   a. Select `run_cms`.
   b. Select Enter the number to turn off the CMS software.
4. Enter the number associated with the **acd_remove** option.
5. Enter the number `(1-7)` of the ACD you want to remove. The system displays the following message:

```
All administration and historical data for this ACD will be DELETED.
Do you want to continue and delete all data for this ACD? (y/n):
```

6. Enter: `Y`. The system displays the following message:

```
Removal of data for this ACD started in the background.
A completion message will be logged in /cms/install/logdir/admin.log.
```

7. Since the ACD is removed in the background, you can turn the CMS software on before the removal is complete.
8. Restart the CMS software:
   a. Enter the number associated with the `run_cms` option.
   b. Enter the option to turn on the CMS software.

**Related links**

Using the CMSADM menu on page 60

# Backing up the file system (backup)

You can use this process to back up the file system. Encryption is supported for CMSADM backups. You can access the backup utility from the command line interface or through an unattended **cron** job. For more details, see CMSADM backup on page 95.

**Important:**

- This option does not back up CMS data. To back up CMS data, you must perform a full maintenance backup in addition to the CMSADM backup. For more information about maintenance backups, see *Administering Avaya Call Management System*.

**Related links**

Using the CMSADM menu on page 60
Backup encryption and other options on page 118

# Installing feature packages (pkg_install)

## About this task

You can use this process to install a feature package, for example LDAP authentication or Dual IP support.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Enter the number associated with the **pkg_install** option. The system displays a list of the feature packages that are not already installed. For example:

```
The CMS Features that can be installed are
1) forecasting
2) external call history
3) multi-tenancy
4) Dual IP
5) LDAP authentication
Enter choice (1-5) or q to quit:
```

4. Enter the number associated with the feature package that you want to install.

**Related links**

Using the CMSADM menu on page 60

# Removing feature packages (pkg_remove)

## About this task

You can use this process to remove a feature package plus all files and database items associated with that feature package.

**Caution:**

- Removing a feature package also removes all files and database data associated with that package.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Turn off the CMS software:
   a. Select `run_cms`.
   b. Select Enter the number to turn off the CMS software.
4. Enter the number associated with the **pkg_remove** option. The system displays a list of the installed feature packages.
5. Enter the number associated with the feature package you want to remove. The system displays a message indicating the feature is removed.
   - For the multi-tenancy feature package, the system displays a menu where you can choose to delete all tenant users or change the tenant users to normal users.

   ```
   Should tenant users be:
   1) deleted
   2) changed to normal users
   Enter choice (1-2) or q to quit:
   ```
6. Restart the CMS software:
   a. Enter the number associated with the `run_cms` option.
   b. Enter the option to turn on the CMS software.

**Related links**

Using the CMSADM menu on page 60

# Turning a feature package on/off (run_pkg)

### About this task

You can use this process to turn an installed feature package on or off.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Enter the number associated with the **run_pkg** option. The system displays a list of CMS features.
4. Enter the number associated with the feature package that you want to turn on or off. The system displays the status of the feature.

**Related links**

Using the CMSADM menu on page 60

# Turning IDS on/off (run_ids)

## About this task

You can use this process to turn IDS on or off.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Enter the number associated with the **run_ids** option.
4. Select the required action:
   - **To turn IDS on:** Enter 1.
   - **To turn IDS off:** Enter 2.

**Related links**

Using the CMSADM menu on page 60

# Turning CMS on/off (run_cms)

## About this task

You can use this process to turn the CMS software on or off.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Enter the number associated with the **run_cms** option.
4. Select the required action:
   - **To turn the CMS on:** Enter 1.
   - **To turn just CMS Off:** Enter 2.
   - **To turn both CMS and IDS off:** Enter 3.

**Related links**

Using the CMSADM menu on page 60

# Switching password aging on/off (passwd_age)

## About this task

Password aging is off by default. You can use this process to turn password aging on/off, and to set the default number of days for aging.

When password aging is on:

- Password aging affects all Linux and CMS users who use the `/usr/bin/cms` shell. However, you can exclude specific users from the password aging policy, see Excluding a user from password aging on page 126.
  - Non-CMS users such as *root*, *root2*, or *informix* do not age.
  - If you are using LDAP, the server running the directory service controls password aging.
- When password aging is on, the system modifies the RHEL policy file `/etc/passwd`.

**Important:**

- To avoid additional password administration, Avaya recommend that you exclude specific users before turning password aging on.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **`cmsadm`**. The system displays the administration menu.
3. Enter the number associated with the **`passwd_age`** option. The output displays the following:

```
1) Turn on password aging
2) Turn off password aging
3) Change password aging interval
or q to quit: (default 1)
```

4. Do one of the following:
   - **To turn password aging on:**

     Enter `1`. CMS prompts you to also enter the number of weeks before passwords expire. You can enter a value between 1 and 52 weeks. If you do not enter a value, CMS sets the default passwords aging to 9 weeks.
   - **To turn password aging off:**

     Enter `2` and then enter `y` to confirm when prompted.
   - **To change the current default password aging period:**

     Enter `3` to change the password current password aging interval and then specify the maximum number of weeks before passwords expire. You can enter a value between 1 and 52.

### Related links

Using the CMSADM menu on page 60

Configuring password aging on page 125

# Controlling ODBC/JDBC database access (dbaccess)

## About this task

By default, the CMS database has open access permissions as a standard feature which allows permission to any CMS login, connecting to CMS through ODBC/JDBC, to view any CMS table.

You can use this process to limit which CMS logins have ODBC/JDBC access to the CMS database.

- Adding a single CMS login to the dbaccess group disables open access permissions for all users who are not members of the dbaccess group.
- 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.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. You need to add each CMS login, allowing ODBC/JDBC access to the CMS database, to the Linux group dbaccess.
   a. Enter `usermod -G dbaccess cmslogin` where cmslogin is the user-id of the specific CMS login to be placed in the group.
   b. Repeat the `usermod` command for each CMS login for which you want to provide CMS database access
3. To check which logins are in the dbaccess group, enter: `cat /etc/group | grep dbaccess`.
4. Enter **`cmsadm`**. The system displays the administration menu.
5. 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,?]
```

6. 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 displays one grant connect message per CMS login, including logins already in the dbaccess group with connect permissions. To remove ODBC/JDBC access permissions for CMS logins, first remove them from the Linux dbaccess group then run dbaccess from the**Avaya Call Management System Administration menu.** menu

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

7. Remove ODBC/JDBC access permissions for CMS logins from the Linux dbaccess group. Enter: `usermod –G “” cmslogin`
8. Enter **cmsadm**. The system displays the administration menu.
9. 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 Linux dbaccess group information is reset to only provide access permissions to members remaining in the Linux dbaccess group.

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

```
usermod –G “” cmslogin1
usermod –G “” cmslogin2
usermod –G “” cmslogin3
```

11. Enter **cmsadm**. The system displays the administration menu.
12. 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,?]
```

13. Enter: `Y`. The process restores public permissions to the CMS database. The system displays messages similar to the following:

```
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.
```

**Related links**

Using the CMSADM menu on page 60

## Configuring a feature package (config_pkg)

You can use `config_pkg` command to configure the LDAP feature. See Installing the LDAP feature package on CMS on page 32.

**Related links**

Using the CMSADM menu on page 60

# Using the CMSSVC menu

This section describes how to use the options of the Avaya Call Management System Services Menu (CMSSVC menu). The CMSSVC menu is for use primarily by Avaya authorized services personnel.

**Related links**

Accessing the CMSSVC menu on page 70
Displaying the authorisation status (auth_display) on page 71
Setting the WebLM server address (weblm_set) on page 72
Turning IDS on/off (run_ids) on page 72
Turning CMS on/off (run_cms) on page 73
Running the CMS initial configuration (setup) on page 73
Display the ACD switch info (swinfo) on page 73
Changing the ACD switch options (swsetup) on page 74
Uninstalling CMS (uninstall) on page 75
Editing the CMS security options (security) on page 76

## Accessing the CMSSVC menu

### About this task

You can use this process to display the CMS Service menu.

- The options displayed in the menu vary depending on the version of CMS.
- You cannot access **cmsadm** or **cmssvc** commands whilst another user or process is running a **cmssvc** setup command. When this occurs, CMS displays a **Please try later, setup is active** error message.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.

```
Avaya(TM) Call Management System Services Menu
Select a command from the list below.
```

```
1) auth_display Display feature authorizations
2) weblm_set Set up the connection to the WebLM
3) run_ids Turn Informix Database on or off
4) run_cms Turn Avaya CMS on or off
5) setup Set up the initial configuration
6) swinfo Display switch information
7) swsetup Change switch information
8) uninstall Remove the CMS rpm from the machine
9) patch_rmv Backout an installed CMS patch
10) back_all Backout all installed CMS patches from machine
11) security Administer CMS security features
Enter choice (1-11) or q to quit:
```

**Related links**

Using the CMSSVC menu on page 70

# Displaying the authorisation status (auth_display)

## About this task

You can use this process to display the authorization status for CMS features.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.
3. Enter the number associated with the **auth_display** option. The system displays the current authorization status of the CMS features and capacities

```
Capability/Capacity Authorization
-------------------- -------------
WebLM/Port/License ID test
CMS release R19
License Duration 02/14/20
forecasting authorized
external call history authorized
multi-tenancy authorized
Dual IP authorized
LDAP authentication authorized
Maximum number of ACDs 8
Simultaneous Avaya CMS Supervisor logins 1600
Number of authorized agents (RTU) 80000
Number of authorized ODBC connections 10
Number of CLInt sessions for Avaya internal use 100
Number of CLInt sessions for non Avaya use 100
FIPS 140-2 mode off
Firewall off
Enhanced Access Security Gateway (EASG) enabled
Disk encryption auto-unlocking enabled
```

**Related links**

Using the CMSSVC menu on page 70

# Setting the WebLM server address (weblm_set)

## About this task

You can use this process to set the address of the WebLM server providing the CMS license.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.
3. Turn off the CMS software:
   a. Select `run_cms`.
   b. Select Enter the number to turn off the CMS software.
4. Enter the number associated with the **weblm_set** option. The system displays the following:

   ```
   Please enter the hostname for the WebLM license server: (default: 10.10.10.10)
   ```

5. Enter the IP address or host name of the WebLM server where the CMS license is installed. The system displays the following:

   ```
   Please enter the CMS server license ID: (default: XXX)
   ```

6. Enter the CMS server license ID. The system displays the following:

   ```
   Web URL is now authorized as https://10.20.30.40:52233/WebLM/LicenseServer.WebLM
   ```

7. Restart the CMS software:
   a. Enter the number associated with the `run_cms` option.
   b. Enter the option to turn on the CMS software.

### Related links

Using the CMSSVC menu on page 70

# Turning IDS on/off (run_ids)

## About this task

You can use this process to turn IDS on or off.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.
3. Enter the number associated with the **run_ids** option.

4. Select the required action:
   - **To turn IDS on:** Enter `1`.
   - **To turn IDS off:** Enter `2`.

**Related links**

Using the CMSSVC menu on page 70

# Turning CMS on/off (run_cms)

## About this task

You can use this process to turn the CMS software on or off.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **`cmssvc`**. The system displays the service menu.
3. Enter the number associated with the **`run_ids`** option.
4. Select the required action:
   - **To turn the CMS on:** Enter `1`.
   - **To turn just CMS Off:** Enter `2`.
   - **To turn both CMS and IDS off:** Enter `3`.

**Related links**

Using the CMSSVC menu on page 70

# Running the CMS initial configuration (setup)

You can use the **`cmssvc`** > **`setup`** command to run the initial configuration of CMS.

- Do not confuse this option with the **`swsetup`** option, which is used to change the switch information.

**Related links**

Using the CMSSVC menu on page 70

# Display the ACD switch info (swinfo)

## About this task

You can use this process to display the current switch options of each ACD.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.
3. Enter the number associated with the **swinfo** option. The system displays a list of ACDs.
4. Select the ACD for which you want to display the switch options. The system displays the following information:
   - Switch name
   - Switch model (release)
   - Local port
   - Remote port
   - Link transport method (TCP/IP)

**Related links**

Using the CMSSVC menu on page 70

## Changing the ACD switch options (swsetup)

### About this task

You can use this process to change the switch options for each ACD.

### Before you begin

- When you change switch parameters, you should also check the parameters in the CMS System Setup: Data Storage Allocation window.
- If you enable Vectoring, you need to allocate space for VDNs and vectors.
- Changing the switch release may change the number of measured entities allowed and also impact the storage allocation for each entity.:

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.
3. Turn off the CMS software:
   a. Select `run_cms`.
   b. Select Enter the number to turn off the CMS software.
4. Enter the number associated with the **swsetup** option. The system displays a list of ACDs.

5. Select the ACD that you want to change.
6. At the prompts, provide the following information:
   - Switch name
   - Switch model (release)
   - Local port assigned to the switch (Avaya recommends that you use 1)
   - Remote port assigned to the switch (Avaya recommends that you use 1)
   - Enter the host name or IP address and TCP port
   - The optional secondary host name or IP address and TCP port if the Dual IP feature has been installed
7. If the switch information is correct, enter: `Y`
8. Restart the CMS software:
   a. Enter the number associated with the `run_cms` option.
   b. Enter the option to turn on the CMS software.

**Related links**

Using the CMSSVC menu on page 70

# Uninstalling CMS (uninstall)

## About this task

You can use this process to uninstall the CMS RPM from the system.

## Before you begin

**Caution:**

Refer to the readme file on the CMS software disc to determine the state of CMS before uninstalling CMS.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **`cmssvc`**. The system displays the service menu.
3. Turn off the CMS software:
   a. Select `run_cms`.
   b. Select Enter the number to turn off the CMS software.

4. Enter the number associated with the **uninstall** option. The system displays messages similar to the following:

```
The following package is currently installed:
cms-r19-XX.X.x86_64
Do you want to remove this package? [y,n,?] ?
```

5. Enter `Y` to uninstall CMS.
6. Accept the default value of y for each prompt. The CMS software is removed.

**Related links**

Using the CMSSVC menu on page 70

# Editing the CMS security options (security)

This section explains how to manage security options.

**Related links**

Using the CMSSVC menu on page 70
Turning FIPS mode on/off on page 76
Turning EASG on/off on page 77
Turning the firewall on/off on page 78
Viewing the firewall configuration on page 80
Disk encryption on page 81

## Turning FIPS mode on/off

### About this task

You can use this process to turn FIPS mode on or off.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.
3. Turn off the CMS software:
   a. Select `run_cms`.
   b. Select Enter the number to turn off the CMS software.
4. Enter the number associated with the **security** option. The system displays the following options:

```
Select one of the following:
1) FIPS 140-2 mode
2) Firewall
3) Enhanced Access Security Gateway (EASG)
4) Disk encryption
Enter choice (1-4) or q to quit:
```

5. Enter the number associated with the **FIP 140-2** option. The system displays the current status of FIPS and a set of options:

```
FIPS 140-2 mode is currently off

Select one of the following
1) Turn on FIPS
2) Turn off FIPS
Enter choice (1-2) or q to quit:
```

6. Enter the number associated with the required option. The next message depends on whether passphrase auto-lock is enabled.

   - **If passphrase auto-unlock is enabled:**

```
Modification of FIPS 140-2 mode requires a change to the kernel. A reboot is
required for the change to take effect.
Would you like to continue? (y/n/q)
```

   - **If passphrase auto-unlock is disabled:**

```
Modification of FIPS 140-2 mode requires a change to the kernel. A reboot is
required for the change to take effect. Access to the system console to enter
the disk encryption passphrase is required on reboot.
Would you like to continue? (y/n/q):
```

     You must enter the passphrase at the system console after rebooting.

7. The system changes the FIPS mode for both ssh and https. After successful configuration of FIPS changes, the system displays the following message:

```
FIPS mode will be (on/off) for both ssh and https. Please wait…
FIPS is now turned on/off.
Are you ready to reboot? (y/n)
```

8. CMS FIPS support changes apply to both ssh and https communications. You must reboot your computer to enable any changes to FIPS mode. Select the required action:

   - If you select `Y`, the following message is displayed.

```
After the reboot, you will need to manually turn on CMS.
Press Enter to continue
Rebooting the system now…
```

   - If you select `N`, the following message is displayed.

```
FIPS mode modifications are being discarded. No change to the kernel has been
made.
```

**Related links**

Editing the CMS security options (security) on page 76

## Turning EASG on/off

### About this task

Enhanced Access Security Gateway (EASG) is a service used by Avaya for remote support access. You can use this process to turn EASG access on or off.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.
3. Enter the number associated with the **security** option. The system displays the following options:

```
Select one of the following:
1) FIPS 140-2 mode
2) Firewall
3) Enhanced Access Security Gateway (EASG)
4) Disk encryption
Enter choice (1-4) or q to quit:
```

4. Enter the number associated with the **Enhanced Access Security Gateway (EASG)** option. The system displays the following messages depending on the status of **EASG**:

```
Select one of the following
1) Disable EASG
2) Enable EASG
3) Display EASG Certificate
Enter choice (1-3) or q to quit: q
```

5. Select the required option:
   - **To enable EASG:** Enter the number associated with **Enabled EASG**.
   - **To disable EASG:** Enter the number associated with **Disable EASG**.

**Related links**

Editing the CMS security options (security) on page 76

### EASG Alarms

When EASG is enabled, the system installs the logs in the `/etc/cron.d` directory with daily scheduled execution. When the threshold reaches expires, the system sends the CMS alarm accordingly.

CMS generates monthly alarms for the 365 day and 180 day expiration notifications, and daily alarms for 30 day and expired notifications.

The certificate expires 15 years from the time it was acquired and can be checked by selecting **cmssvc** > **security** > **Enhanced Access Security Gateway (EASG)** > **Display EASG Certificate**.

## Turning the firewall on/off

### About this task

You can use this process to turn the firewall service on or off.

For information about port usage, see *Port Matrix for Avaya Call Management System*.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.
3. Enter the number associated with the **security** option. The system displays the following options:

```
Select one of the following:
1) FIPS 140-2 mode
2) Firewall
3) Enhanced Access Security Gateway (EASG)
4) Disk encryption
Enter choice (1-4) or q to quit:
```

4. Enter the number associated with the **Firewall** option. The system displays one of the following messages depending on the status of Firewall:

```
Firewall for ipv4 is currently on
Firewall for ipv6 is currently on
```

```
Firewall for ipv4 is currently off
Firewall for ipv6 is currently off
```

**Note:**

Note: The status between ipv4 and ipv6 must be consistent with each other. If not, you must consider restarting or stopping the firewall.

The system also displays the following message:

```
Select one the following
1) Set/reset firewall configuration using CMS provided iptables/ip6tables
2) Start/restart firewall
3) Stop firewall
Enter choice (1-3) or q to quit:
```

5. Enter the number associated with **Set/reset firewall configuration using CMS provided iptables/ip6tables** option. The system displays the following message:

```
In addition to port 22 for ssh,
Do you want to open port 8443 for CMS Web client https connections? (y/n)
Do you want to open port 50000 for ODBC/JDBC connections? (y/n)
Do you want to open port 50001 for ODBC/JDBC connections? (y/n)
```

A `/cms/install/security/OpenPorts` file is created for Avaya Professional Services and customers to add ports to be excluded from the firewall. If the file contains valid port numbers, the system displays the following message:

```
The following port(s) specified in /cms/install/security/OpenPorts will also be
open for connections:
Port Usage
-----------
514 # CMS HA
```

If you change the default settings CMS gets the `ssh port from /etc/ssh/sshd_config` file. The default is port 22

CMS gets the https port from `/opt/cmsweb/tomcat/conf/server.xml` file. The default is port 8443.

CMS configures both `/etc/sysconfig/iptables and /etc/sysconfig/ip6tables` files to be used by the Linux iptables/ip6tables services for firewall protection. The system displays the following message:

```
Firewall configuration is completed.
Do you want to restart the firewall now? (y/n)
```

**Note:**

You can choose to maintain iptables/ip6tables and bypass option 1.

6. Do one of the following:
   a. Enter the number associated with the Start/restart firewall option after you change the firewall configuration files manually or through CMS. The system displays one of the following messages:

```
iptables: Applying firewall rules: [ OK ]
ip6tables: Applying firewall rules: [ OK ]
```

```
Firewall for ipv4 is currently off
Firewall for ipv6 is currently off
```

   b. Enter the number associated with **`Stop firewall`** option. The system displays one of the following messages:

```
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Flushing firewall rules: [ OK ]
iptables: Unloading modules: [ OK ]
ip6tables: Setting chains to policy ACCEPT: filter [ OK ]
ip6tables: Flushing firewall rules: [ OK ]
ip6tables: Unloading modules: [ OK ]
```

```
Firewall for ipv4 is currently off
Firewall for ipv6 is currently off
```

A root user can obtain the current firewall configuration by running the following commands:

```
iptables -L -n --line-numbers
ip6tables -L -n --line-numbers
```

**Related links**

Editing the CMS security options (security) on page 76

## Viewing the firewall configuration

When firewall is on, you can view the status of the IPv4 and IPv6 firewalls using the **`iptables`** and **`ip6tables`** commands respectively.

### IPv4 firewall status

The following is an example firewall status shown following an **iptables** status command:

```
Table: filter
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
2 ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
3 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
4 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:8443
5 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:50000
6 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:50001
7 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:1556
8 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:13724
9 LOGGING all -- 0.0.0.0/0 0.0.0.0/0
Chain FORWARD (policy ACCEPT)
num target prot opt source destination
1 LOGGING all -- 0.0.0.0/0 0.0.0.0/0
Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
Chain LOGGING (2 references)
num target prot opt source destination
1 LOG all -- 0.0.0.0/0 0.0.0.0/0 limit: avg 2/min burst 5 LOG
flags 0 level 4 prefix `IPTables-Dropped: '
2 REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited
```

### IPv6 firewall status

The following is an example firewall status shown following an **ip6tables** status command:

```
Table: filter
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT all ::/0 ::/0 state RELATED,ESTABLISHED
2 ACCEPT all ::/0 ::/0
3 ACCEPT tcp ::/0 ::/0 tcp dpt:22
4 ACCEPT tcp ::/0 ::/0 tcp dpt:8443
5 ACCEPT tcp ::/0 ::/0 tcp dpt:50000
6 ACCEPT tcp ::/0 ::/0 tcp dpt:50001
7 ACCEPT tcp ::/0 ::/0 tcp dpt:1556
8 ACCEPT tcp ::/0 ::/0 tcp dpt:13724
9 LOGGING all ::/0 ::/0
Chain FORWARD (policy ACCEPT)
num target prot opt source destination
1 LOGGING all ::/0 ::/0
Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
Chain LOGGING (2 references)
num target prot opt source destination
1 LOG all ::/0 ::/0 limit: avg 2/min burst 5
LOG flags 0 level 4 prefix `IP6Tables-Dropped:'
2 REJECT all ::/0 ::/0 reject-with icmp6-admprohibited
```

**Related links**

Editing the CMS security options (security) on page 76

## Disk encryption

By default, CMS no longer encrypts CMS data disks and partitions using LUKS encryption. Instead is uses the default encryption provided by the cloud service providers or virtual machine hosting CMS.

**Related links**

Editing the CMS security options (security) on page 76

# Maintaining WebLM licenses

## Activating the license for a CMS server

### About this task

**Important:**

Each CMS deployment must have its own license file on a WebLM Release 8.0 or later server and must use Centralized Licensing. Enterprise licensing is not supported for CMS. That is, multiple CMS deployments cannot share one license file.

### Before you begin

Get the following information:

- SAP order number
- WebLM server host ID

**Note:**

The SAP order number and the WebLM server host ID must be listed under the same Company ID.

### Procedure

1. In a browser window, navigate to the PLDS site: https://plds.avaya.com
2. Log on to PLDS using your customer ID and password.
3. Navigate to **Assets** > **View**Entitlements. PLDS displays the Search Entitlements screen.
4. Search for your license entitlement using one of the following criteria:
   - SAP order number
   - Sold to number
   - License activation code

   You can also use Advanced Search to find a license entitlement.
5. Click **Search Entitlements**.PLDS displays the known license entitlements based on the search criteria.
6. For the customer’s entitlement record, click **Options** > **Activate** . PLDS displays a list of possible entitlements.
7. Select the entitlement for CMS release for which you are installing or upgrading.
8. Click **Activate**.PLDS displays the Search License Hosts screen. The available license hosts for the Company ID are displayed on this screen.

**Note:**

You can also download a license file and install the file manually.

9. Select one of the displayed license hosts or create a new host by clicking **Add a License Host**.
10. Click **Next**. PLDS displays a **registration summary** screen.
11. Click Next. PLDS displays the **Activate Entitlements** screen.
12. Select the quantity of each entitlement you want to activate.
13. Click **Next**.

**Note:**

Add notes for the activation, if needed.

14. Click **Finish**.

# Installing a license file on a WebLM server

## About this task

Avaya products use WebLM Release 8.0 or later to manage product licenses obtained using PLDS. For CMS licensing, the customer must use either a standalone WebLM server or have the WebLM server installed on a coresident Avaya product, such as Avaya Aura® System Manager

Licenses installed for WebLM must support SHA256 digital signatures and a 14-character host ID.

**Important:**

You must use Centralized Licensing when licensing CMS. Enterprise licensing is not supported for CMS. That is, multiple CMS deployments cannot share one license file. After enabling Centralized Licensing, you must assign every license file to the license ID in WebLM.

For more information about installing license files, see the following documents:

- *Administering Avaya Aura® System Manager*
- *Administering standalone Avaya WebLM*

## Before you begin

Ensure that the XML license file is present in the computer. Use the uninstall functionality of WebLM to remove any existing license file from the WebLM server before you install a new license file. The system displays an error message if an older license file is still available. For a centralized license file, the system automatically overwrites the older license file during installation. If you experience problems while installing the license file, see *Administering standalone Avaya WebLM*.

## Procedure

1. Log on to the standalone WebLM web console or the Avaya Aura® System Manager console with administrator privilege credentials.
2. In the navigation pane, click **Install license**.

3. On the Install license page, click **Choose File** and browse to the directory of the XML license file that you saved on your computer.
4. Read the terms and conditions and click **Accept the License Terms & Conditions**
5. Click **Install**.WebLM displays a message on successful installation of the license file. The installation of the license file might fail for reasons, such as the digital signature on the license file is invalid. If you get such an error, request PLDS to redeliver the license file. Another error could be caused by the current capacity use exceeds the capacity in the installed license.
6. Enable Centralized Licensing as describe in WebLM documentation. With Centralized Licensing, you must assign every license file to the license ID in WebLM.
7. Click **New**.
8. Enter a name you want to assign to that CMS.
9. Select the license file you want to associate with that CMS.

# Managing alarms and error logs

The system creates a new license.log in the /cms/env/lm directory to record the status whenever CMS checks the license usage against WebLM. The system stores the error and informational logs for up to 45 days.

Below are conditions for the system to trigger log messages into the CMS elog:

- When a new license violation occurs
- When a license violation clears
- When license status changes
- Daily reminder when CMS is in license error or restricted mode

The Always on Management (AOM) subsystem is configured to map license elog messages into alarms. Based on AOM settings, the system forwards the alarms through the socket connection or SNMP agent to Initialization and Administration System (INADS) and customer network management system.

**Note:**

Currently, CMS does not support clearing of existing alarms

CMS has three levels of alarms:

- Warning: The system triggers a warning alarm when CMS is in the License Error mode.
- Minor: The system triggers a minor alarm when the server enters the License Error Mode.
- Major: The system triggers a major alarm when the server enters the License Restricted Mode. In the License Restricted mode, CMS has limited functionality.

## Warning messages in error mode

The system issues warning messages when CMS is in the License Error mode. In the License Restricted mode, CMS has limited functionality.

The following are the list of possible of violations:

- Cannot access WebLM server
- Cannot obtain CMS license
- CMS license expired
- Invalid CMS version
- Number of ACDs exceed limit
- Number of agents exceed limit
- Number of supervisor log-in exceeds limit
- Number of JDBC/ODBC sessions exceed limit
- Number of CLIint sessions exceed limit

When CMS is either in License Error or License Restrictive Mode, the system displays a warning message.

# Warning message in the License Error mode

Insert content for the first section.

For License Error Mode the system displays the following warning message for **cmssvc/cmsadm** in the menu items:

```
WARNING: CMS is in License Error Mode
License violation(s): xxxxx.
You have until xxxxx to fix your errors before CMS enters License Restricted Mode
and
becomes unusable.
```

## Warning message in the License Restricted mode

For License Restricted Mode the system displays the following warning message for **cmssvc/cmsadm** in the menu items:

```
WARNING: CMS is in License Restricted Mode
18 License violation(s): xxxxx.
19 Access to CMS is restricted.
```

# Backing up and restoring WebLM

The CMS instance does support backing up or restoring the current license state. To restore CMS from a catastrophic loss, you must restart the CMS instance. The system gets the license data from WebLM and determines the license state.

# Upgrading to WebLM

The software upgrade process extracts the package installation information from previous installations. However, the process discards the authorization information. CMS requires access to WebLM 8.0 or later for CMS license.

# Managing personal data in CMS

CMS stores the following types of personal data:

- Call center agent information.
- CMS user information.
- Phone numbers dialed by individuals placing calls into the call center.
- Phone numbers dialed by agents placing calls outside the call center.

The call center agent information and CMS user information is for employees of the company using CMS. The type of personal data CMS stores is limited to that information that facilitates standard employee work operations.

The information related to individuals calling into the call center is specific to digits dialed. The information related to agents calling outside the call center is also specific to digits dialed. CMS provides logs and tools that help you manage personal data in CMS.

For more information about how CMS manages personal data, see Avaya Call Management System.

# Deleting phone numbers from CMS

### About this task

You can delete sensitive phone numbers from the CMS database. This is a one-time operation. If a phone number you delete from the CMS database is later dialed again by an individual dialing into the call center or an agent dialing outside the call center, the phone number is inserted into the CMS tables again.

### Before you begin

The delete operation is logged in the following log file: `/cms/db/log/phone_delete.log`

**Note:**

Since ECH data is not retained for more than 24 hours, that data is not subject to rules about personal data removal. Phone numbers are not deleted from ECH.

### Procedure

1. Log on to Linux as a root user.

   **Note:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

2. Enter the following command: `/cms/toolsbin/delete_phone <PhoneNumber>`. Where `<PhoneNumber>` is the dialed phone number you want to delete.

## Personal data log files

CMS logs changes to agent and CMS user personal data.

- All add, delete, and modify actions for user data are logged in the following location: `/cms/db/log/user_chg.log`
- All add, delete, and modify actions for agent names are logged in the following location: `/cms/db/log/agname_chg.log`

# Configuring the encryption passphrase

### About this task

CMS automatically encrypts the data partitions on the storage disk drive during an OVA deployment. Encryption is not optional — the data partitions on the storage disk drive are always encrypted. A newly-deployed or upgraded system is assigned two default encryption passphrases.

You can choose from either of the following default encryption passphrases:

- CMSdefault
- CMSsvcdefault

The customer must decide whether they will require an encryption passphrase to be entered on the console after the system has shut down and rebooted. This includes shutdowns for administrative or maintenance procedures such as turning FIPS on and off, CMSADM restore, LAN restore, RPM update, software upgrades, and regular maintenance reboots as recommended by Avaya. It also includes unplanned shutdowns such as a system crash.

**Caution:**

If the customer requires an encryption passphrase after a shutdown, that passphrase must be entered on the system console. The passphrase cannot be entered remotely after the system has rebooted. You can work around this requirement by temporarily disabling the encryption passphrase before doing the reboot, but you must remember to enable the encryption passphrase after the reboot is complete. However, if the system crashes, there is no workaround and the encryption passphrase must be entered on the system console.

**Important:**

Whether the customer requires the encryption passphrase after a shutdown and reboot, the customer must change the passphrase from the default to a passphrase known only to the customer and Avaya services. The customer must record the new encryption passphrase in a safe, secure location.

### Before you begin

Consult with the customer to find out whether they want to require an encryption passphrase after a shutdown and reboot. The customer can always change this decision.

### Procedure

1. Log on as root.

**Important:**

You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

2. Enter: `cmssvc`. The system displays the following menu:

```
Avaya(TM) Call Management System Services Menu
Select a command from the list below.
1) auth_display Display feature authorizations
2) weblm_set Set up the connection to the WebLM
3) run_ids Turn Informix Database on or off
4) run_cms Turn Avaya CMS on or off
5) setup Set up the initial configuration
6) swinfo Display switch information
7) swsetup Change switch information
8) uninstall Remove the CMS rpm from the machine
9) patch_rmv Backout an installed CMS patch
10) back_all Backout all installed CMS patches from machine
11) security Administer CMS security features
Enter choice (1-11) or q to quit:
```

3. Enter the number that corresponds to the security command. The system displays the following menu:

```
Select one of the following:
1) FIPS 140-2 mode
2) Firewall
3) Enhanced Access Security Gateway (EASG)
4) Disk encryption
Enter choice (1-4) or q to quit:
```

4. Enter the number that corresponds to the `Disk encryption` command. The system displays the following menu:

```
Disk encryption auto-unlocking is enabled.
Select one of the following
1) Change encryption passphrase
2) Enable auto-unlocking
3) Disable auto-unlocking
Enter choice (1-3) or q to quit:
```

5. To change the encryption passphrase, do the following steps:

**Important:**

Whether the customer requires the encryption passphrase after a shutdown and reboot, the customer must change the passphrase from the default to a passphrase known only to the customer and Avaya services. The customer must record the new encryption passphrase in a safe, secure location.

a. Enter the number that corresponds to the `Change encryption passphrase` command. The system displays the following message:

```
Select one of the following
1) Primary encryption passphrase
2) Secondary encryption passphrase
Enter choice (1-2) or q to quit:
```

b. Select the primary or secondary encryption passphrase option. The system displays the following message:

```
Enter current encryption passphrase:
```

c. Enter the current encryption passphrase and press **Enter**.The system displays the following message:

```
Enter new encryption passphrase:
```

d. Enter the new encryption passphrase and press **Enter**. The system displays the following message:

```
Re-enter new encryption passphrase:
```

e. Re-enter the new encryption passphrase and press **Enter**.The system displays messages similar to the following example:

```
Changing passphrase for disk partition /dev/sda3 ...
Changing passphrase for disk partition /dev/sda7 ...
Changing passphrase for disk partition /dev/sda10 ...
Changing passphrase for disk partition /dev/sda11 ...
```

f. Repeat these steps for the second passphrase.

6. To enable encryption auto-unlocking, do the following steps:

a. Enter the number that corresponds to the Enable auto-unlocking command. The system displays the following message:

```
Enter an existing encryption passphrase:
```

b. Enter the current encryption passphrase and press **Enter**. The system displays messages similar to the following example:

```
Adding auto-unlocking key file to partition /dev/sda3 ...
Adding auto-unlocking key file to partition /dev/sda7 ...
Adding auto-unlocking key file to partition /dev/sda10 ...
Adding auto-unlocking key file to partition /dev/sda11 ...
Changing reboot setting ...
Auto-unlocking enabled successfully.
```

7. To disable encryption auto-unlocking, do the following steps:

**Caution:**

If the customer requires an encryption passphrase after a shutdown, that passphrase must be entered on the system console. The passphrase cannot be entered remotely after the system has rebooted. You can work around this requirement by temporarily disabling the encryption passphrase before doing the reboot, but you must remember to enable the encryption passphrase after the reboot is complete. However, if the system crashes, there is no workaround and the encryption passphrase must be entered on the system console.

a. Enter the number that corresponds to the `Disable auto-unlocking` command. The system displays the following message:

```
Enter an existing encryption passphrase:
```

b. Enter the current encryption passphrase and press **Enter**. The system displays messages similar to the following example:

```
Changing reboot setting ...
Removing auto-unlocking key file from partition /dev/sda3 ...
Removing auto-unlocking key file from partition /dev/sda10 ...
Removing auto-unlocking key file from partition /dev/sda7 ...
Removing auto-unlocking key file from partition /dev/sda11 ...
```

# Updating the LDAP authentication package configuration

An installed LDAP authentication package may require configuration updates to:

- Align with source LDAP Active Directory configuration changes, for example, a Bind password.
- Enable or disable LDAP encryption.
- Update an encryption certificate.

## LDAP authentication configuration

### Before you begin

Complete the following LDAP worksheet. This worksheet identifies the Active Directory server and encryption certificate information that you must enter when installing the LDAP package.

| Active Directory Server information | Example | Your Value |
|---|---|---|
| Enable optional encrypted LDAP connection (TLS/SSL) | yes, no | |
| Path to certificate exported from LDAP server – must be provided when LDAP encryption=yes | /tmp/my_AD_cert.cer | |
| Windows Active Director server IP Address or Fully Qualified Domain Name An FQDN must be provided when LDAP encryption=yes | 10.20.30.40 or http://ADServer.company.com | |
| Port number for the Active Directory server | 389 (default for TCP) 636 (default for TLS/SSL)<br>Or specific value from your AD server | |

## Installing an LDAP encryption certificate

### About this task

Use this procedure if you plan to add LDAP encryption or update an existing LDAP encryption certificate. You must export the Active Directory certificate from the Windows Active Directory

server. This procedure exports the Certificate Authority Active Directory certificate and installs the certificate on the CMS server.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmssvc**. The system displays the service menu.
3. Turn off the CMS software:
   a. Select `run_cms`.
   b. Select Enter the number to turn off the CMS software.
4. Do the procedure Installing an LDAP encryption certificate. <<<You what>>>
5. After importing the certificate, you can update an existing installation of the LDAP feature package to use the new certificate.

## Updating the LDAP authentication configuration

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Enter the number associated with the **pkg_install** option. The system displays a list of the feature packages that are not already installed. For example:

```
The CMS Features that can be installed are
1) forecasting
2) external call history
3) multi-tenancy
4) Dual IP
5) LDAP authentication
Enter choice (1-5) or q to quit:
```

4. Select `LDAP Authentication`. The system displays a message similar to the following example:

```
Existing Configuration:
LDAP network connection is encrypted.
Secure(TLS) LDAP certificate is installed. Expiration date: XX/XX/XXXX
LDAP server IP Address or Fully Qualified Domain
Name:ADServer.company.com
Port Number for the LDAP server: 636
Bind Distinguished Name: CN=Administrator,CN=Users,DC=CPOD,DC=com
Bind Distinguished Password: *******
Base Distinguished Name: ou=CMSUsers,dc=CPOD,dc=com
LDAP network connection is encrypted.
Secure(TLS) LDAP certificate is installed. Expiration date: XX/XX/XXXX
Do you want LDAP connections to be encrypted(TLS/SSL)(y/n)?
(default: y):
```

**Note:**

If the LDAP connection is not using encryption, the system does not display the first two lines about encryption and certificates.

5. Do one of the following:
   - If encryption is not currently being used and you do not plan to add encryption at this time, type `n` and continue with Step 10.
   - If encryption is currently being used and you want to continue using encryption, type `y` and continue with Step 6.
6. When an encryption certificate exists, the system displays the following message:

   ```
   A valid Active Directory certification is currently installed.
   Do you want to replace it and install a new certificate (y/n):
   ```

7. Do one of the following:
   - If you want to continue using the same certificate, press `N` and continue with Step 9.
   - If you want to replace the existing certificate with a new certificate, press `N` and continue with Step 7.
8. The system displays the following message:

   ```
   Enter the full path to the certificate file exported from your LDAP server
   (eg:/tmp/my_AD_cert.pem):
   ```

9. Type the location where you have imported the new certificate and press `Enter`.
10. The system displays the following message:

    ```
    Enter the LDAP server IP Address or Fully Qualified Domain Name:
    ```

11. Type the IP address or FQDN of the LDAP server and press `Enter`.

    **Important:**

    When the LDAP connection is encrypted (TLS/SSL), you must enter an FQDN.

    The system displays the following message:

    ```
    Enter the port number of the LDAP server (default: 636):
    ```

12. Enter the Windows server Active Directory port number and press `Enter`. The system displays the following message:

    ```
    Enter the Bind Distinguished Name(eg: CN=Adm,OU=Users,DC=example,DC=com):
    ```

13. Type the Bind Distinguished Name and press Enter. For example, type: `CN=Administrator,CN=Users,DC=CPOD,DC=com`. The system displays the following message:

    ```
    Enter the password for the Bind Distinguished Name:
    ```

14. Type the password for the **Bind Distinguished Name** and press `Enter`. The system displays the following message:

    ```
    Retype the password for the Bind Distinguished Name:
    ```

15. Type the password for the **Bind Distinguished Name** again. It must be the same as the previous entry, or you will be required to re-enter the password twice again. Press `Enter`.The system displays the following message:

    ```
    Enter the Base Distinguished Name for CMS user authentication:
    ```

16. Type the Base Distinguished Name for CMS user authentication and press `Enter`.For example, type: `ou=CMSUsers,dc=CPOD,dc=com`. The system displays a message similar to the following example:

    ```
    LDAP network connection is encrypted.
    Secure(TLS) LDAP certificate path: /storage/my_ldap_cert.pem
    LDAP server IP address or Fully Qualified Domain Name: host.example.com
    Port Number for the LDAP server: 636
    Bind Distinguished Name: CN=Administrator,CN=Users,DC=CPOD,DC=com
    Bind Distinguished Password: *******
    Base Distinguished Name: ou=Users,dc=CPOD,dc=com
    Are the above inputs correct? (y/n, or q to quit): (default:n):
    ```

17. Do one of the following:

    - Type `Y` if the settings are correct.
    - Type `n` if the settings are not correct. The system will step you through each setting and allow you to change any of the settings.

18. The system verifies access to the Active Directory server and Based Distinguished Name, then displays the following message on successful installation of the package:

    ```
    LDAP authentication package installed.
    ```

19. If the installation failed, a message will display requesting input for the failed verification item(s). Input messages will continue until the inputs are successfully verified. To correct, verify the Active Directory Server values and accurate input.

20. Restart the CMS software:

    a. Enter the number associated with the `run_cms` option.

    b. Enter the option to turn on the CMS software.

# Removing the LDAP authentication package

### About this task

You can remove the LDAP authentication feature. When you remove all LDAP, the system remove all configuration attributes. The system converts all CMS users with the LDAP authorization to regular CMS users. The password must be set for these users as new CMS user.

When you Remove the LDAP authentication, it results in removal of the LDAP feature and conversion of CMS users with LDAP authentication to CMS server authentication.

### Before you begin

Turn off CMS.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Turn off the CMS software:
   a. Select `run_cms`.
   b. Select Enter the number to turn off the CMS software.
4. Type the number associated with the `pkg_remove` option and press `Enter`. The system display varies depending on the packages currently installed:

```
The CMS Features that can be removed are
1) forecasting
2) LDAP authentication
```

5. Type the number that corresponds to the `LDAP Authentication` package and press `Enter`. The system displays the following message:

```
Removing LDAP authentication will result in full removal of the LDAP feature and
conversion of CMS users with LDAP authentication to CMS server authentication.
Do you want to continue (y/n, or q to quit)
```

6. Type `Y` and press `Enter`. The system displays the following message:

```
LDAP authentication removed.
```

7. Restart the CMS software:
   a. Enter the number associated with the `run_cms` option.
   b. Enter the option to turn on the CMS software.

# Backing up data

There are two types of data backup available for CMS:

- CMSADM backup
- Maintenance backup

**Caution:**

If you do not perform regular backups of your data and you have a system failure, data will be lost and cannot be recovered. More frequent backups will increase your chances of not losing data. It is up to you to determine how much data loss you can tolerate if you choose to not back up your data more frequently.

CMS supports CMS backups to multiple backup devices. You cannot run simultaneous backups of any type, even if multiple backup device types are administered.

CMS can back up data and restore data while the data collection remains on. This helps minimize data loss. However, once a CMSADM backup starts, new login attempts using CMS Supervisor or the ASCII interface are blocked.

CMS maintenance backups only save CMS data (administration and historical) and the CMS data for each ACD. You can do maintenance backups using CMS Supervisor. Avaya recommends that you perform full maintenance backups weekly and incremental maintenance backups daily.

## CMSADM backup

The CMSADM file system backup saves all local file systems on the computer onto a backup device, including:

- System files and programs
- CMS programs

**Important:**

The CMSADM backup does not save CMS database tables. During the CMSADM backup, no users can log in to CMS, other than those already logged in before the backup was started.

## When to do a CMSADM backup

Do the CMSADM file system backup at the following times:

- After the CMS is provisioned to backup the RHEL system files, system programs and CMS configuration data placed on the computer by Avaya Services provisioning personnel. These CMSADM backups can be to tape, a USB storage device or a network mount point and should also be saved and not reused or overwritten. CMS supports CMS backups to multiple backup devices. Avaya is no longer providing CMS backup tapes with CMS servers. If a customer chooses to use tape drives to back up the customer's CMS data then the customer is responsible for purchasing the tape drive and any supplies needed to operate the tape drive. The customer is responsible for backing up CMS after the system has been provisioned. The customer must store the CMSADM backup in a safe place in case the system needs to be restored.
- After the CMS server is provisioned. This backup contains the RHEL system files and programs and CMS configuration data placed on the computer by Avaya Services provisioning personnel. These tapes should also be saved and not reused.

  In addition, field technicians should do a CMS full maintenance backup before they turn a new system over to the customer. For more information, see *Administering Avaya Call Management System*.
- Before and after the CMS software is upgraded (usually performed by a field technician)
- Once a month (performed by the customer).

**Important:**

You must document the CMS load number and backup/restore device information to aid in disaster recovery of CMS.

You must document the CMS load number and backup/restore device information to aid in disaster recovery of CMS. `rpm -q cms`

Below are examples of the type of information that needs to be saved:

| CMS host name | CMS Load Number |
|---|---|
| digger<br>Your CMS server | cms-r19-X.X.X.x86_64 |

| CMS hostname | Backup/Restore Device Type (Tape/USB/ Network) | Backup/Restore Device Path | Backup/Restore Device Name | Description |
|---|---|---|---|---|
| digger<br><br>Your CMS server | USB | /CMS_Backup | USB_ digger | USB backup<br>for digger |

**Important:**

Unlike tape devices, USB storage devices and network mount points must be monitored to ensure they are accessible. Timetables and Backup/Restore Devices using USB storage devices and network mount points must be able to access these media sources to function properly. Remember to remount all non-tape media sources, used by CMS, after any reboot of the system.

CMS maintenance backups only save CMS data (administration and historical) and the CMS data for each ACD. You can do maintenance backups using CMS Supervisor. For more information, see *Administering Avaya Call Management System*. Avaya recommends that you do full maintenance backups weekly and incremental maintenance backups daily.

# When to do a maintenance backup

CMS maintenance backups only save CMS data (administration and historical) and the CMS data for each ACD. You can do maintenance backups using CMS Supervisor. For more information, see *Administering Avaya Call Management System*.

Avaya recommends that you do full maintenance backups weekly and incremental maintenance backups daily.

# Data space requirements for CMS backups

## Calculating data space requirements for CMSADM backups

### Procedure

1. Log on as root to Linux.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

2. Run the following command: `df -Th`. The system displays information similar to the following example:

```
Filesystem Type Size Used Avail Use% Mounted on
devtmpfs devtmpfs 7.8G 0 7.8G 0% /dev
tmpfs tmpfs 7.8G 0 7.8G 0% /dev/shm
tmpfs tmpfs 7.8G 113M 7.7G 2% /run
tmpfs tmpfs 7.8G 0 7.8G 0% /sys/fs/cgroup
/dev/sda2 ext4 9.8G 1.6G 7.7G 18% /
/dev/sda1 ext4 546M 106M 400M 21% /boot
/dev/sda6 ext4 87G 2.7G 80G 4% /storage
/dev/sda9 ext4 16G 45M 15G 1% /tmp
/dev/sda8 ext4 26G 240M 24G 1% /var
/dev/dm-0 ext4 32G 49M 30G 1% /export/home
/dev/dm-1 ext4 12G 1.8G 9.3G 16% /opt
/dev/dm-2 ext4 9.8G 354M 8.9G 4% /cms
tmpfs tmpfs 1.6G 0 1.6G 0% /run/user/0
cms-store:/store nfs4 2.2T 1.5T 554G 74% /nfsbu
```

3. Add the disk space from the Used column for all of the ext4 filesystems, except for the /storage and /tmp directories. In this example, that would include the following directories:
   - /
   - /boot
   - /var
   - /export/home
   - /opt
   - /cms
4. Calculate the space you will need, for example:

| Directory | Used space |
|---|---|
| / | 1.6 GB |
| /boot | 106 MB |
| /var | 240 MB |
| /export/home | 49 MB |
| /opt | 1.8 GB |
| /cms | 354 MB |
| TOTAL | 4.15 GB |

The df -Th command gives a current snapshot of disk space usage of the CMS server. You must run additional checks periodically to see if your storage needs have changed to ensure that you have enough backup space.

## Calculating data space requirements for CMS full maintenance backups

### Procedure

1. Log on to Linux as *root*.

**Important:**

- If using a remote connection, you cannot directly log on as *root*. Instead, log on using an administered CMS user ID and then then use `su - root` to log on with root privileges.

2. Run the following command to set the Informix environment: **`./opt/informix/bin/setenv`**
3. Run `onstat -d`
4. Use the output generated from running this command to estimate how much database space is required for a CMS full maintenance backup. The data in this table is dynamic and changes as database space is used.

**Note:**

- Bytes to GB conversion factor = 1,073,741,824.
- Full Maintenance Backup compression ratio = 30 (approximation). The `onstat -d` command gives a current snapshot of disk space usage of the CMS server.
- You must run additional checks periodically to see if your storage needs have changed to ensure that you have enough backup space.

# Backing up CMS to a USB storage device

## Configuring and connecting a USB storage device

The customer is responsible for the proper configuration of the USB storage device and connectivity to the CMS server. CMS servers running RHEL only support USB Removable Mass Storage devices formatted using the ext4 file system. RHEL can detect USB storage devices formatted with other file system types but CMS only supports the ext4 file system. If your USB storage device is formatted with any file system type other than ext4, you need to reformat the device. RHEL does not support mounting for an unformatted USB storage device.

You cannot use CMS to manage the file system on the USB device or NFS mounts. CMS will continue to write backups to the device until all space is used up. You are responsible for all file rotation activities. In this manner, a customer with an extra large NFS area could save 20 copies of the CMSADM backup for their system, whereas a customer with a small USB stick might only want to keep 2 copies on that device.

**Important:**

For large CMS configurations, avoid using USB storage devices for data backups. You are responsible for ensuring that the CMS server detects the USB storage device and users can perform read and write operations to and from the USB storage device. This document provides information as a reference to aid in troubleshooting USB storage device recognition issues. For help with resolving any USB storage device issues, contact your system administrator. Ensure you can write to and read from the installed USB storage devices before performing any maintenance or CMSADM backups.

# Verifying the USB storage device is recognized by the CMS server

## About this task

Output from the fdisk command provides information that is needed to mount the USB storage device.

## Procedure

1. Insert the USB storage device.
2. Enter: `fdisk -l`. The output of the `fdisk` command is similar to the following:

```
Disk /dev/sda: 598.9 GB, 598879502336 bytes
255 heads, 63 sectors/track, 72809 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0002a1a9
Device Boot Start End Blocks Id System
/dev/sda1 * 1 73 586341 83 Linux
/dev/sda2 74 1318 9999565+ 83 Linux
/dev/sda3 1318 2563 10000000 83 Linux
/dev/sda4 2563 72810 564257326 f W95 Ext'd (LBA)
/dev/sda5 2563 3559 7999999+ 82 Linux swap
/dev/sda6 3559 26659 185546874+ 83 Linux
/dev/sda7 26659 30643 31999999+ 83 Linux
/dev/sda8 30643 33879 25999999+ 83 Linux
/dev/sda9 33879 35871 15999999+ 83 Linux
/dev/sda10 35871 37358 11937499+ 83 Linux
/dev/sda11 37358 72810 284772950+ 83 Linux
Disk /dev/sdb: 64.7 GB, 64692944896 bytes
64 heads, 32 sectors/track, 61696 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

**Note:**

On Linux® Operating System systems, the USB disk path is similar to `/dev/sdx` as shown in this output.

3. Determine the size and available disk space of a USB storage device. Refer to *Administering Avaya Call Management System* for information on how to determine the amount of space needed for a maintenance backup of data.

**Note:**

Do not run this command if a backup is running since the device is already under heavy use.

4. Enter: `df -kl`. The output of the `df -kl` command is the following:

```
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/sda2 9842412 2389400 6953036 26% /
tmpfs 8142556 204 8142352 1% /dev/shm
/dev/sda1 577096 43340 504440 8% /boot
/dev/sda3 9842848 472048 8870800 6% /cms
/dev/sda7 31497112 181064 29716052 1% /export/home
/dev/sda10 11750104 725392 10427840 7% /opt
```

```
/dev/sda6 182634796 846752 172510704 1% /storage
/dev/sda9 15748504 178188 14770320 2% /tmp
/dev/sda8 25591516 284664 24006856 2% /var
/dev/sdb 62185452 3819768 55206852 7% /CMS_Backup
```

**Note:**

If multiple USB storage devices are installed but the system does not display some devices with the df -kl command, then the USB storage device is probably not formatted properly. Contact your system administrator to correctly configure the USB storage device. The information below is for reference only and should only be performed by experienced personnel.

**Caution:**

Formatting a USB storage device will overwrite all data on the USB storage device and all data will be lost. Be sure you are certain you want to remove all data on the USB storage device. If you do not want to remove the data on the USB storage device, replace the USB storage device with a different USB device that can be formatted, and restart this procedure from Step 2.

a. To change to the root directory, enter: `cd /`

b. To create the `ext4` filesystem on the USB storage device, enter: `mkfs -t ext4 /dev/sdx`, where, `/dev/sdx` is the disk path found with the fdisk command.

**Warning:**

No warnings are given about overwriting old data. Do not run this command unless you are sure you do not want any data from the USB stick.

5. Mount the USB storage device by performing the following steps:

   a. Create the mount point if the mount point does not exist, enter: `mkdir /{mount_point}`

   b. To mount the USB storage device, enter: `mount /dev/sdx /{mount_point}`. where `/dev/sdx` is the disk path

   c. To verify the USB storage device is mounted, enter: `ls -l /{mount_point}`The USB storage device directory should display the following message:

   ```
   drwx------. 2 root root 16384 <timestamp> lost+found
   ```

6. Verify files can be written to and read from the USB storage device by creating a file on the USB storage device and accessing the file from the USB storage device.

**Note:**

You need to update read and write permissions for the backup directories just created so that system and data backups can be performed by any user authorized to run these backups.

# Mounting a USB storage device

## Procedure

1. Insert the USB storage device.
2. To mount the USB storage device, enter: `mount {mount_point}`

**Note:**

Avaya recommends that you create the USB mount points in the root directory to prevent problems due to administrators misplacing or forgetting mount point information.

# Unmounting a USB storage device

## Procedure

To unmount the USB storage device, enter: `umount /CMS_Backup`

**Note:**

USB storage devices used by timetables and backups must be mounted for them to function properly. Remember to remount all non-tape Backup/Restore Devices after any reboot of the system.

# Administering a backup or restore device for a USB storage device

## Before you begin

A backup or restore device must be administered before a CMSADM or Maintenance backup to a USB storage device can be performed

**Note:**

The Backup/Restore Devices screen limits the length of the path name that can be entered so keep the directory names as short as possible.

## Procedure

1. Open the CMS main menu and select **Maintenance** > **Backup/Restore Devices**. The system displays the **Maintenance Backup/Restore Devices** screen.
2. Enter a **Device name**
3. Enter the Path of the USB storage device. For example, `/CMS_Backup`
4. Enter a **Description**.
5. Select the Device Type **Other**.
6. Select **Add**. If the USB storage device path entered does not exist, a message similar to the following will be displayed:

```
Path not valid for type "Other".
Press return to continue:
```

To resolve this issue, be sure the USB storage device is accessible and the directory path exists.

7. To view the administered backup devices, select **List devices**.

## Doing a CMSADM backup to a USB storage device

### Procedure

1. Verify that:
   - The computer is in a multi-user state (2 or 3). To check whether you are in the multi-user state, enter `who -r`
   - The USB storage device is installed and configured.
   - To determine the size and available disk space of the USB storage device, enter: `df -kl`

   **Caution:**

   Ensure the USB storage device has enough space for this CMSADM system backup
2. Log on as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.
3. Enter: `cmsadm`. The system displays the **Avaya Call Management System Administration** Menu
4. Enter the number associated with the backup option. Depending on the configuration of your system, the system displays the following options:

   ```
   Choose a backup device:
   1) Tape
   2) Other
   Enter choice (1-2) or q to quit:
   ```
5. Select the number for the **Other** option.
6. Enter the Path of the USB storage device (the path must not be located on the CMS server).
7. The CMSADM back up begins. To monitor the progress of the CMSADM backup, enter: `tail -f /cms/install/logdir/backup.log`

   When the backup is completed, the system displays messages similar to the following:

   Call Management System

   ```
   9399920 blocks
   Backup Verification
   9399920 blocks
   Backup file is located at /CMS_Backup/CMSADM-rxxxx.x-120330010438-trex
   ```
8. Avaya recommends that CMSADM backup files written to USB storage devices be saved to another location for disaster recovery.

# Doing a CMS maintenance backup to a USB storage device

## Procedure

1. From the CMS main menu select **Maintenance** > **Back Up Data**.

   The **Maintenance Backup Data** screen is displayed.

2. Select **List devices** to view the available backup devices.
3. Press `F5` to close the list of devices window
4. Enter the **USB storage Device** name.
5. Select **Run** to do the **Maintenance Back Up** of Data.

   If the Verification field is set to `Y`, the system displays the following message:

   ```
   WARNING: Your named device "{mount_point}" is not a tape storage
   Device and you have requested a tape verification. If
   you choose to continue, the verify request will
   be ignored.
   Enter yes to continue or no to cancel.
   Enter y or Y for yes, n or N for no:
   ```

6. Select `Y` to continue
7. The Maintenance back up of data begins. You can monitor the progress of the data backup by entering: `tail -f /cms/maint/backup/back.log`. Messages similar to the following will be written to the `/cms/maint/backup/back.log` when the backup successfully completes.

   ```
   state: 1
   /cms/install/bin/compress_backup successfully finished: <Day>,<timestamp>
   error:
   status: Last backup finished >, <timestamp>.
   state: 0
   ```

8. Avaya recommends that CMS Full Maintenance backup files written to USB storage devices be saved to another location for disaster recovery.

# Checking the contents of the CMSADM backup to USB

## About this task

The system lists the files on the USB storage device so you can determine if the backup has saved the correct information or verify that a particular file has been saved.

**Note:**

It can take a long time to display the file names on the USB storage device.

## Procedure

1. Insert the USB storage device.
2. To list the files on the USB storage device, enter: `ls -l /{mount_point}`. For example, `ls -l /CMS_Backup`

3. To list the individual CMSADM files on the USB storage device, enter the following command on a single line: `cpio -ivct -C 10240 -I /{mount_point}/ <CMSADM_filename> | more`,where `<CMSADM_filename>` is the filename of the CMSADM backup file of interest.

   For example, `cpio -ivct -C 10240 -I /CMS_Backup/ CMSADM-R21.0.0.0Laa.s-240528111315-cmsvm9.gpg | more`

   **Note:**

   The name of the CMSADM backup file identifies the following:

   - Type of backup: `CMSADM`
   - CMS version at the time of the backup: `r21.0.0.0`
   - Date of the backup: `240528` in *yymmdd* format.
   - Unique identifier of the backup: `111315`
   - CMS hostname: `cmsvm9`

4. After you have seen the files you are looking for or have confirmed that data on the USB storage device is accurate, press `Delete` to stop the display.

# Backing up CMS to a network mounting point

## Configuring and connecting to a network mount point

The customer is responsible for the proper configuration of network mount points and connectivity to CMS.

**Important:**

Contact your system administrator before creating any shared mount points or network mount points. It is the responsibility of the customer to determine if any security violations will be made by creating share points and allowing other systems on the network to access the share points. Creating and sharing mount points should only be performed by experienced personnel.

It is the responsibility of the customer to ensure that CMS detects the network mount point and users can do read and write operations to and from the network mount point. This document provides information as a reference to aid in troubleshooting network mount point recognition issues but you should NOT contact Avaya to resolve any issues with your network mount points. Instead, contact your system administrator to resolve any network mount point issues. Be sure you can write to and read from network mount points before performing any Maintenance or CMSADM backups.

## Configuring an NFS server

**Important:**

When using NFS for backups you must use NFS Version 4 (v4). When upgrading from an older version of CMS that supports an older version of NFS, you must upgrade your NFS setup to NFS v4 after you upgrade your system.

The customer is responsible for the proper configuration and connectivity between the NFS server and CMS server. The CMS server does not permit a CMSADM backup and a Maintenance backup to be performed simultaneously, even if multiple backup device types are administered. The following points must be kept in mind while using NFS mounted directories:

- The NFS mount point must be accessible from the CMS server.
- The NFS server must have enough disk space for the backup of data.
- The directory path used when administering an NFS Back Up Device must exist on the NFS server.

The following procedures will provide basic information about configuring a NFS server and CMS server to support NFS backups and restores:

- If the network server is Solaris, continue with Configuring a mount point on a Solaris 10 NFS server on page 105.
- If the network server is RHEL, continue with Mount point configuration on a Linux NFS server on page 108.
- If the network server is on a VMware deployment, continue with Mount point configuration on a VMware datastore on page 112.

**Note:**

You cannot use CMS to manage the filesystem on the USB device or NFS mounts. CMS will continue to write backups to the device until all space is used up. The customer is responsible for taking care of all file rotation activities. In this manner, a customer with an extra large NFS area could save 20 copies of the CMSADM backup for their system, whereas a customer with a small USB stick might only want to keep 2 copies on that device.

## Configuring a mount point on a Solaris 10 NFS server

**Important:**

When using NFS for backups you must use NFS Version 4 (v4). When upgrading from an older version of CMS that supports an older version of NFS, you must upgrade your NFS setup to NFS v4 after you upgrade your system.

Do the following steps on the Solaris network server.

**Note:**

These steps are not performed on the CMS server itself. They are performed on the NFS server which must be a separate, non CMS, customer provided Solaris computer.

The following table shows variables used in these procedures and the definition of those variables.

| Variable | Definition |
|---|---|
| *network_server_mt_pt_dir* | Network server directory that will be mounted from the CMS server as an NFS mount point. |
| *CMS_FQDN* | Fully qualified domain name of the CMS server. |

1. To create the network mount point, enter: **mkdir /network_server_mt_pt_dir**

   Example:

   **mkdir /store**

2. Set the permissions for the network_server_mt_pt_dir, enter: **chmod 755 /network_server_mt_pt_dirchown nobody:nobody / network_server_mt_pt_dir**

   **Note:**

   Later, if you are unable to write to the network mount point on the CMS server indicated by a “Permission denied” message on the CMS server, you will need to set the owner and group to nfsnobody. Enter: **chown nfsnobody:nfsnobody / network_server_mt_pt_dir**

3. To share the Solaris network server, edit /etc/dfs/dfstab and add a line with the Solaris network server directory that will be shared:

   a. Enter:

      **vi /etc/dfs/dfstab**

   b. Append the Solaris network mount point information to the bottom of the file: **share -F nfs -o rw=CMS_FQDN /network_server_mt_pt_dir**

      Example:

      **share -F nfs -o rw=lucy.acme.avaya.com /store**

   c. Write and save the file.

4. Enable NFS network server:

   **svcadm -v enable -r network/nfs/server**

5. To verify the network service is online, enter:

   **svcs | grep nfs**

6. Restart NFS to activate the share, enter:

   **svcadm restart network/nfs/server**

7. To share all administered mount points, enter:

   **shareall**

8. To see what mount points are being shared, enter:

   **share**

9. To unshare a single mount point, enter:

   **unshare /network_server_mt_pt_dir**

10. To unshare all administered mount points, enter:

    **unshareall**

Do the following steps on the CMS server.

**Note:**

The Backup/Restore Devices screen limits the length of the path name that can be entered so keep the directory names as short as possible.

The following table shows variables used in these procedures and the definition of those variables.

| Variable | Definition |
|---|---|
| *network_server_mt_pt_dir* | Network server directory where the CMS server will write and read backup data |
| *NS_backup_dir* | CMS directory for mounting the Network server directory |

1. To create the network mount point directory, enter:

   **mkdir /NS_backup_dir**

   Example:

   **mkdir /nfsbu**

2. To add the Solaris network mount point to **/etc/fstab**, do the following steps:

   a. Enter:

      **vi /etc/fstab**

      **Warning:**

      Be very careful when you make changes to the **/etc/fstab** file. You must not change existing entries in this file as the system can fail to boot properly as a result of the changes you make.

   b. Append the Solaris network mount point information to the bottom of the file. **network_server:/network_server_mt_pt_dir /NS_backup_dir nfs rw,bg,soft,intr,nosuid 0 0**

      Example:

      **cms-store:/store /nfsbu nfs rw,bg,soft,intr,nosuid 0 0**

   c. Write and save the file.

3. To mount the network server mount point directory, enter:

   **mount /NS_backup_dir**

4. To change to the network server mount point directory, enter:

   **`cd /NS_backup_dir`**

5. To list the contents of the network server mount point directory, enter: **`ls -`**

   **Note:**

   The contents of this directory should be the same as that of the directory contents of the actual network server mount point directory.

6. To determine the size and available disk space of the network server mount point directory, enter: **`df -k`**

   **Note:**

   There should be adequate space to backup the data. The data compression rate is very high on most systems. Refer to *Administering Avaya Call Management System* for information on how to determine the amount of space needed for a maintenance backup of data.

7. To unmount a network server mount point directory, enter: **`umount /NS_backup_dir`**

   **Note:**

   Network server mount points used by timetables and backups must be mounted for them to function properly. Remember to remount all non-tape Backup/Restore devices after unmounting.

8. Continue with Administering a Backup/Restore Device for a network mount point on page 115

## Mount point configuration on a Linux NFS server

There are two distinct procedures in this task. The first procedure is done on the Linux NFS server. The second procedure is done on the CMS server.

**Important:**

When using NFS for backups you must use NFS Version 4 (v4). When upgrading from an older version of CMS that supports an older version of NFS, you must upgrade your NFS setup to NFS v4 after you upgrade your system.

### Configuring mount point for the Linux NFS server

#### About this task

These steps are not performed on the CMS server itself. They are performed on the NFS server which must be a separate, non-CMS, customer-provided RHEL computer.

The following table shows variables used in these procedures and the definition of those variables.

| Variable | Definition |
|---|---|
| *network_server_mt_pt_dir* | Network server directory that will be mounted from the CMS server as an NFS mount point |
| *CMS_FQDN* | Fully qualified domain name of the CMS server |

## Procedure

1. To create the network mount point, enter: **mkdir /network_server_mt_pt_dir**

   **mkdir /store**

2. Set the permissions for the `network_server_mt_pt_dir`, enter: **chmod 755 /network_server_mt_pt_dirchown nobody:nobody / network_server_mt_pt_dir**

   **Note:**

   Later, if you are unable to write to the network mount point on the CMS server indicated by a “Permission denied” message on the CMS server, you will need to set the owner and group to nfsnobody. Enter: **chown nfsnobody:nfsnobody / network_server_mt_pt_dir**

3. To allow other systems to access the network mount point, do the following steps:

   a. Enter: **vi /etc/exports**

   b. Append the RHEL network mount point information to the bottom of the file: **/ network_server_mt_pt_dir CMS_FQDN(rw,sync)**

   **/store lucy.dr.avaya.com(rw,sync)**

   c. Write and save the file.

   **Note:**

   Later, if you are unable to mount a network mount point on the CMS server with the failure “special device does not exist”, you might need to make an additional update. First, confirm the mount directory exists on this NFS server. If the mount directory exists, re-execute Steps 3a, 3b, 3c, and then restart the NFS service in Step 5.

   In Step 3b, change the previously added line to:

   **/network_server_mt_pt_dir CMS_FQDN(rw,sync,fsid=0)**

   Example:

   **/store lucy.dr.avaya.com(rw,sync,fsid=0)**

4. To configure NFS and portmap to start on reboot:

   a. Log on as root.

**Important:**

You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

b. Enter: **ntsysv**

c. A GUI interface is started. Scroll through the list provided and verify that the nfs and portmap options are selected. These two options should be marked with an x.

d. Enter TAB to highlight **OK**.

e. Click **OK**.

5. For a Linux NFS server using a pre-RHEL Version 7 OS, start the NFS service by doing the following steps:

**Note:**

When the /etc/exports file is changed, it is necessary to stop and start the NFS server.

a. If the NFS service is not running, enter: **/etc/init.d/nfs start**

b. If the NFS service is running, enter: **/etc/init.d/nfs restart**

c. To verify the network service is running, enter: **service nfs status**

6. For a Linux NFS server using an RHEL Version 7 or later OS, start the NFS service by doing the following steps:

**Note:**

When the /etc/exports file is changed, it is necessary to stop and start the NFS server.

a. To start or restart the NFS service, enter: **systemctl restart nfs**

b. To verify the network service is running, enter: **systemctl status nfs**

## Configuring mount point for the CMS server

### About this task

The following table shows variables used in these procedures and the definition of those variables.

| Variable | Definition |
|---|---|
| *network_server_mt_pt_dir* | Network server directory where the CMS server will write and read backup data |
| *NS_backup_dir* | CMS directory for mounting the Network server directory |

**Note:**

The Backup/Restore Devices screen limits the length of the path name that can be entered so keep the directory names as short as possible.

## Procedure

1. To create the network mount point directory, enter: **`cd /mkdir /NS_backup_dir`**

   **`mkdir /nfsbu`**

2. To add the RHEL network mount point to `/etc/fstab`, do the following steps:

   a. Enter: **`vi /etc/fstab`**

   **Warning:**

   Be very careful when you make changes to the `/etc/fstab` file. You must not change existing entries in this file as the system can fail to boot properly as a result of the changes you make.

   b. Append the network mount point information to the bottom of the file: **`network_server:/network_server_mt_pt_dir /NS_backup_dir nfs rw,bg,soft,intr,nosuid 0 0`**

   **`cms-store:/store /nfsbu nfs rw,bg,soft,intr,nosuid 0 0`**

   c. Write and save the file.

3. To mount the network server mount point directory, enter: **`mount /NS_backup_dir`**

   **Note:**

   If the mount failure “special device does not exist” is encountered, do the following steps:

   a. On the NFS Server, redo Steps 3a, 3b, 3c, and 5. Follow the Step 3 Note.

   b. On the CMS server, redo step 2, replace step b with: **`network_server:/ /NS_backup_dir nfs rw,bg,soft,intr,nosuid 0 0`**

   **`cms-store:/ /nfsbu nfs rw,bg,soft,intr,nosuid 0 0`**

4. To change to the network server mount point directory, enter: **`cd /NS_backup_dir`**

5. To list the contents of the network server mount point directory, enter: **`ls -l`**

   **Note:**

   The contents of this directory should be the same as that of the directory contents of the actual network server mount point directory.

6. To determine the size and available disk space of the network server mount point directory, enter: **`df -k`**

   **Note:**

   There should be adequate space to backup the data. The data compression rate is very high on most systems. Refer to *Administering Avaya Call Management System* for information on how to determine the amount of space needed for a maintenance backup of data.

7. To unmount a network server mount point directory, enter: **umount /NS_backup_dir**

**Note:**

Network server mount points used by timetables and backups must be mounted for them to function properly. Remember to remount all non-tape Backup/Restore devices after unmounting.

## Mount point configuration on a VMware datastore

You can configure a mount point on a VMware deployment to do CMSADM and maintenance backups to a VMware datastore. Avaya recommends that you create a datastore dedicated to CMS backups and label it for CMS backups so it can be easily found if you have to do a restore.

**Caution:**

To create a mount point on a VMware deployment, you cannot create the mount point on the same datastore that the CMS software and database are installed. If the CMS datastore and the backups are on the same datastore and that datastore fails, you cannot restore the system.

### Adding a hard disk to use as the backup datastore

#### Procedure

1. Start the vSphere client software on your PC.
2. Log on to the vSphere client software.
3. Select **Getting Started** > **Edit virtual machine settings**.

   The Virtual Machine Properties page is displayed.
4. Select **Add**.

   The Add Hardware page is displayed.
5. On the Device Type page, select Hard Disk and click Next.
6. On the Select a Disk page, select **Create a new virtual disk** and click **Next**.
7. On the Create a Disk page, set the following options:
   - For the **Disk Size** option, decide on how much data you have to back up and set the disk size to that amount. 200 GB is a good starting point.
   - Select **Thin Provision**.
   - Select **Specify a datastore or datastore cluster**.
8. Select **Browse** to display the available datastores or datastore clusters.
9. Select the datastore or datastore cluster created for CMS backups.

**Caution:**

Do not select the same datastore that the CMS software and database are installed. If the CMS datastore and the backups are on the same datastore and that datastore fails, you cannot restore the system.

10. Click **OK**.

    The selected datastore or datastore cluster is displayed.

11. Click **Next**.
12. On the Advanced Options page, select **Independent and Persistent**.
13. Click **Next**.
14. On the Ready to Complete page, verify that the settings are correct.
15. Click **Finish**.

    The new virtual hard disk is displayed on the Virtual Machine Properties page.

16. Write down the name of the disk as shown in the **Disk File** field. This information is used when creating a mount point and when restoring the system. For example: `[backup-datastore] Call Management System R19/Call Management R19.vmdk`

## Configuring the mount point for a VMware virtual disk

### Procedure

1. Open a console terminal window.
2. Log on to the console.
3. Enter: **`fdisk -l`**

   The output of the **`fdisk`** command is similar to the following:

```
Disk /dev/sda: 644.2 GB, 644245094400 bytes
255 heads, 63 sectors/track, 78325 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
 I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000842e4
Device    Boot    Start    End    Blocks        Id    System
/dev/sda    *  1        73    583676+                83    Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2            73    1379     10485756+     83      Linux
/dev/sda3          1379    2684     10485756+     83      Linux
/dev/sda4          2684    78326       607589376     f    W95
Ext'd (LBA)
/dev/sda5          2684    3729     8388604+      82    Linux swap
/dev/sda6          3729    5003     10239996+     83    Linux
/dev/sda7          5003    9181     33554428+     83    Linux
/dev/sda8             9181    12575    27262972+    83    Linux
/dev/sda9          12575      14663    16777212+    83    Linux
/dev/sda10         14663      16222    12517372+    83    Linux
/dev/sda11         16222      78326    498847744    83    Linux
```

**Note:**

On Linux® systems, the virtual disk path is similar to what is shown above as `/dev/sdb`.

4. Determine the size and available disk space of the new virtual hard disk. For more information, see *Administering Avaya Call Management System* on how to determine the amount of space needed for a maintenance backup of data.
5. Enter: **df -kl**

   **Note:**

   Do not run this command if a backup is running since the virtual hard disk is already under heavy use.
6. Mount the virtual hard disk by performing the following steps:
   a. Create the mount point if the mount point does not exist. Enter: **mkdir /MountPoint**

      **mkdir /CMS_Backup**
   b. To mount the virtual hard disk, enter: **mount /dev/sdX /MountPoint**

      where **/dev/sdX** is the path for the virtual hard disk.

      **mount /dev/sdb /CMS_Backup**
   c. Enter the following commands to create the file system:

      **cd /**

      **mkfs -t ext4 /dev/sdX**

      where /dev/sdX is the path for the virtual hard disk.

      **mkfs -t ext4 /dev/sdb**
   d. To verify the USB storage device is mounted, enter: **ls -l /MountPoint**

      **ls -l /CMS_Backup**

      The virtual hard disk directory should display the following message: `drwx------. 2 root root 16384 <timestamp> lost+found`
   e. Enter the following command after you have mounted the file system to confirm it is set up properly: **df -kl**

      The output of the df -kl command is similar to the following:

```
Filesystem     1K-blocks    Used    Available    Use%
Mounted on
/dev/sda2     10190132    1280812    8385036    14%      /
tmpfs         8166828        0        8166828
0%      /dev/shm
/dev/sda1     558108         30884    498044     6%       /boot
/dev/sda3     10190132    327688     9338160    4%       /cms
/dev/sda7     32896876    49332    31169824     1%       /
```

```
export/home
/dev/sda10    12189612    995764    10567980    9%       /opt
/dev/sda6     9948008    2924396    6511616    31%       /
storage
/dev/sda9     16382884    61776    15482248    1%         /tmp
/dev/sda8     26704120    101180    25239792    1%         /var
/dev/sdb     206293688    60684    195747244    1%         /
CMS_Backup
```

7. Verify that files can be written to and read from the virtual hard disk by creating a file on the virtual hard disk and accessing the file from the virtual hard disk.

   **Note:**

   You need to update read and write permissions for the backup directories just created so that system and data backups can be performed by any user authorized to run these backups.

8. Add the following line at the end of `/etc/fstab` to automatically reset the mount point if the system reboot occurs:

   **`/dev/sdb /CMS_Backup ext4 defaults 1 2`**

## Administering a Backup/Restore Device for a network mount point

### About this task

The user must administer a Backup/Restore device before a CMSADM or Maintenance backup to a network mount point can be performed.

### Procedure

Open the CMS main menu and select **Maintenance** > **Backup/Restore Devices**. The Maintenance Backup/Restore Devices page is displayed.

a. Enter a device name.

b. Enter the path of the network mount point.

   **`/NS_backup_dir/CMS_hostname`**

   Example: `/nfsbu/digger`

   **Note:**

   The `/NS_backup_dir/CMS_hostname` directory must exist on the network server.

c. Enter a description.

d. Select the device type **Other**.

e. Select **Add**.

   If the directory does not exist on the network server a message similar to the following will be displayed:

```
Path not valid for type “Other”.
Press return to continue:
```

To resolve this issue be sure the network server is mounted and the directory exists on the network server.

f. To view the administered backup devices, select **List devices**.

## Checking the contents of the CMSADM backup to a network mount point

### About this task

The system lists the files on the network mount point so you can determine if the backup has saved the correct information or verify that a particular file has been saved.

**Note:**

It can take a long time to display the file names on a network mount point.

To check the contents of the CMSADM backup to a network mount point:

### Procedure

1. To list the files on the network mount point, enter: **`ls –l /NS_backup_dir/CMS_hostname`**
2. To list the individual CMSADM files on the network mount point, enter the following command on a single line: **`cpio -ivct -C 10240 -I /NS_backup_dir/CMS_hostname/<CMSADM_filename> | more`**

   where <CMSADM_filename> is the filename of the CMSADM backup file of interest.

   **`cpio -ivct -C 10240 -I /nfsbu/digger/ CMSADM-r19aa.w-120717150230-digger | more`**

   where the name of the CMSADM backup file identifies the following:

   Type of backup: **`CMSADM`**

   CMS version at the time of the backup: **`r19aa.w`**

   Date of the backup: **`120717 (yymmdd)`**

   Unique identifier of the backup: **`150230`**

   CMS host name: **`digger`**

   The system displays a list of files.
3. After you have seen the files you are looking for or have confirmed that data on the network mount point is accurate, press `Delete` to stop the display.

## Doing a CMSADM backup to a network mount point

### Procedure

1. Verify that:
   - The computer is in multi-user state (2 or 3). To check whether you are in the multi-user state, enter: **`who -r`**

- The network directory is installed and configured.
- To determine the size and available disk space of the network mount point, enter: **df -k**

**Caution:**

Ensure the network mount point has enough space for this CMSADM system backup.

2. Log on as root.

**Important:**

You cannot directly log on as root from a remote connection. You must log on using an

3. Enter: **cmsadm**

   The Avaya Call Management System Administration Menu is displayed.

4. Enter the number associated with the backup option.

   Depending on the configuration of your system, the system displays the following options:

```
Choose a backup device:
1) Tape
2) Other
Enter choice (1-2) or q to quit:
```

5. Enter the number associated with the backup option.
6. Select the number for the Other option.
7. Enter the path of the mounted CMS (the path must not be located on the CMS server).**/NS_backup_dir/CMS_hostname**

   /nfsbu/digger

8. The CMSADM back up begins. To monitor the progress of the CMSADM backup, enter: **tail -f /cms/install/logdir/backup.log**

   When the backup is completed, the system displays messages similar to the following:

```
===== Begin backup <timestamp>
Converter started <timestamp>
Converter completed successfully <timestamp> xxxxxx blocks
===== Finished backup <timestamp>
```

9. Avaya recommends that you save CMSADM backup files written to network directories to another location for disaster recovery.

## Doing a CMSADM backup to a network mount point

### Procedure

1. Verify that:
   - The computer is in multi-user state (2 or 3). To check whether you are in the multi-user state, enter: **who -r**
   - The network directory is installed and configured.

- To determine the size and available disk space of the network mount point, enter: **df -k**

**Caution:**

Ensure the network mount point has enough space for this CMSADM system backup.

2. Log on as root.

**Important:**

You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su- root` to log on with root privileges.

3. Enter: **cmsadm**

The **Avaya Call Management System Administration Menu** is displayed.

## Backup encryption and other options

You can encrypt CMSADM backups. Run `/cms/install/bin/backup -h` to view the available backup options. For example:

```
[root@cmsvm12 x]# /cms/install/bin/backup -h
/cms/install/bin/backup options:
         -b  batch mode : no interaction
         -E  Skip encryption
         -t  Tape backup device  (equivalent to answering 1 to 'Choose a backup device'
prompt)
         -o  Other backup device (ie, not tape) (equivalent to answering 2 to 'Choose a
backup device' prompt)
         -p  /full/path/of/backup/location - implies device is other (not tape) - do
not specify a tape device
         -s  /path/to/passphrase-file - supply passphrase for GPG encryption without
interactive prompting
         -h  Print this message and quit.

[root@cmsvm12 x]# /cms/install/bin/backup -p /backup -s /root/secret
```

### Encrypted backup files

Encrypted backups use the `.gpg` file extension as indicated in the following example:

```
# To list the contents of an encrypted cmsadm backup do:
# - As root user on CMS server with cmsadm backup USB / NFS mounted / accessible
gpg -d /path/to/CMSADM-R21.0.0.0Laa.s-240528112310-server.gpg | cpio -tv -C 10240 | less
```

# Powering off CMS on a virtual machine

### About this task

Use this procedure to shut down CMS and the virtual machine. Shut down the system when you do maintenance on the virtual machine hardware.

### Procedure

1. Log on as root at the console.

2. Enter **shutdown -h 0**

   The system displays a message like the following:

   ```
   Broadcast message from root@example
    (/dev/pts/0) at 20:13 ...
   The system is going down for halt NOW!
   ```

# Starting up CMS on a virtual machine

### About this task

Start the virtual machine and CMS. Do this after you have done maintenance on the virtual system hardware.

### Procedure

Depending on the type of platform hosting the virtual machines, do one of the following:

- If running on a VMware host platform, do the following:
  a. Open a browser to the vSphere vCenter host URL, and log in.
  b. Click **Hosts and Clusters** or **VMs and Templates**.
  c. In the left pane, select the CMS virtual machine.
  d. Click **Actions**, and select **Power On**.
- If running on a KVM host platform, do the following:
  a. Open a browser to the KVM hypervisor, and log in.
  b. Click **Virtual machines**.
  c. To display the CMS virtual machine details, click the name of the CMS virtual machine.
  d. To start the virtual machine, click **Run**.

# Adding disk storage space to a CMS virtual machine

### About this task

You can use the procedures in this section to add disk storage space to a medium or large CMS virtual machine. You need to add disk storage space if the CMS server was not allocated the recommended maximum disk storage space when installed.

The recommended maximum disk storage space is:

- **Medium server configuration:** 1200 GB for VMware and 400 GB for KVM.
- **Large server configuration:** 1800 GB for VMware and 1000 GB for KVM.

**Caution:**

**Small server configuration:** Do not add extra disk storage space to a small server configuration. Adding disk storage space will not affect the service but may impact system performance.

**Warning:**

**All server configurations:**

- Do not change any other resource settings. Changing allocated resources impacts the performance, capacity, and stability of the CMS virtual machine.
- To run at full capacity, the server configuration must match the resource requirements outlined in the *Deploying Avaya Call Management System* document. Any deviation from the resource requirements is at the customer's risk.

### Before you begin

- Check whether IDS is installed on the server and that IDS is turned on.
- Determine the current disk size.
- Power off the CMS server.

### Related links

Adding additional disk storage to a VMware server on page 120
Adding disk storage space to a KVM server on page 121
Attaching the newly added disks to the Informix database on page 121

# Adding additional disk storage to a VMware server

### Procedure

1. Use a browser to log in to the vSphere Web Client.
2. On the vSphere Web Client home page, select **Hosts and Clusters** or **VMs and Templates**.
3. In the left pane, select the CMS virtual machine.
4. Click **Actions**, and select **Edit Settings**.
5. In the **Edit Settings** window, click **ADD NEW DEVICE**.
6. From the drop-down list, select **Hard Disk**.
7. Select **New Hard disk**, and click to expand.
8. Enter the recommended additional disk storage space in the **Size** field:
   - **Medium server configuration:** 400 GB.
   - **Large server configuration:** 1000 GB.
9. Click **Disk Provisioning**, and select **Thick Provision**.

**Caution:**

Customers using their VMware systems can use **Thin Provisioning** at their own risk.

10. Select **OK**.
11. Power on the CMS server.

**Related links**

Adding disk storage space to a CMS virtual machine on page 119

# Adding disk storage space to a KVM server

## Procedure

1. Log in to the KVM hypervisor web URL.
2. Click **Virtual machines**.
3. To display the CMS virtual machine details, click the name of the CMS virtual machine.
4. In the **Disks** section, click **Add disk**.
   a. Enter the appropriate disk file information.
   b. In the **Size** field, enter the recommended additional disk storage space.
   c. Select `qcow2` as the format.
   d. Click **additional options**, and in the **Cache** field, select **directsync**.
   e. Click **Add**.
5. Power on the CMS server.

**Related links**

Adding disk storage space to a CMS virtual machine on page 119

# Attaching the newly added disks to the Informix database

## Procedure

1. Log in to the CMS server as a root user.
2. Ensure that the IDS service is running.
3. To add the new disk to the Informix database, enter **`/opt/informix/bin/dbinit.sh add_disks`**
4. Verify that the disks were added successfully. If the procedure fails, contact Avaya support.

**Related links**

Adding disk storage space to a CMS virtual machine on page 119

# Changing the system date and time

This section describes how to change the system date and time. For example, a change due to daylight savings time.

## Checking the RHEL system date and time

### About this task

To verify that the system time is correct:

### Procedure

1. Enter: **`date`**
2. If the system time is correct there is no need to proceed further with this procedure. If the system time is not correct, continue with Setting the system date and time on page 122.

## Setting the system date and time

### About this task

Do the following steps to change the Linux system time:

### Procedure

1. Turn off the CMS software.
2. Log on as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.
3. Enter the root password.
4. Turn off ntp time synchronization. **`timedatectl set-ntp 0`**
5. Set the time and date by entering: **`timedatectl set-time 'yyyy-mm-dd HH:MM'`**

   For Example:

   - yyyy (year): Entering the year is optional. Enter the year, with all four digits (for example, 2019).
   - mm (month): Enter the month (numeric). Range: 1-12 (1=January, 2=February, and so on).
   - dd (day): Enter the day of the month. Range: 1-31
   - HH (hour): Enter the hour of day, military time. Range: 00-23.
   - MM (minute): Enter the minute of the hour. Range: 00-59.
6. Restart system time date demon. **`systemctl restart systemd-timedated`**

7. Continue with Changing the time zone on page 123.

## Changing the time zone

### Procedure

1. Log on to the system as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

2. Check which time zone your machine is currently using. Enter: **`date`**

   The output of the date command is shown in the following example:

   ```
   Mon 10 Jun 12 21:15:08 PST 2019
   ```

   In this example, the current time zone of the system is PST.

3. Determine the time zone region. Use the following command, replacing the example America, with your actual time zone region: **`timedatectl list-timezones | grep America`**

   Choose the specific time zone region.

4. Set the time zone region. From the list of time zone regions displayed, use the following command, replacing America/Denver, with your actual time zone region name: **`timedatectl set-timezone "America/Denver"`**

5. Set the hardware clock to UTC. Enter: **`timedatectl set-local-rtc 0`**

6. Restart system time date demon.

   **`systemctl restart systemd-timedated`**

# Working with CMS patches

This section provides procedures for maintaining patches for CMS.

## CMS patch requirements

The three occasions when you may have to install CMS patches are:

- During a factory installation
- Immediately after upgrading the CMS software
- In the field on an existing system to correct a problem with the original software.

### Loading patches after an upgrade:

If you are loading patches immediately after upgrading your system, it is best to turn off the CMS software until you have the patches installed. The patches have different prerequisites for installation. Some require that the CMS software be turned off, others require that data collection be turned off, and still others require the CMS software to be in single-user mode. To be absolutely safe, and to help the upgrade proceed as quickly as possible, turn off the CMS software.

### Loading patches as a bug fix:

If you are loading patches as part of a factory installation or on an existing system in the field without upgrading your base load, you can install the patches without turning the CMS software off. The system will display a message if you need to do anything special to accomplish the load.

The CMS patch readme file lists the run-level requirements for each patch.

**Note:**

Call the National Customer Care Center or your product distributor to have authorizations installed.

Installation of all available patches is recommended. If you believe that you should not be installing a particular patch, call the National Customer Care Center or consult with your product distributor before deciding to omit installation of a patch.

# Installing CMS patches

### About this task

Customers should contact their Avaya support organization or business partner regarding the installation of patches for Linux systems.

In the file names shown in the procedure:

- Replace the **xx.y** string with the load name for the patch, for example, **fa.b.**
- Replace the **{n}** with the patch number for that load, for example, **3**.

### Procedure

1. Download `r19xx.y_cmsp{n}-l.bin to /tmp` on the CMS server.
2. Download `r19xx.y_cmsp{n}-l.md5` to / (the root directory) on the CMS server.
3. Enter the following commands to check the md5 sum of the downloaded file: **cd /md5sum r19xx.y_cmsp{n}-l.bin**
4. Verify that the md5 sum matches what was downloaded in the `.md5` file.
5. Turn off CMS.
6. Enter the following command to install the patch: **./ r19xx.y_cmsp{n}-l.bin**

   Follow the prompts to install the patch.
7. Turn on CMS.

## Removing CMS patches

### About this task

To remove CMS patches:

### Procedure

1. Log on as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.

2. Enter: **`cmssvc`**

   The **CMSSVC** menu is displayed.

3. Enter the number associated with the **patch_rmv** option.

   The system lists the patches that are installed on the system and prompts you to select a patch.

4. Type the name of the patch that you want to remove exactly as it is displayed in the list, and press `Enter`.

   The system asks you to verify the removal.

# Configuring password aging

Password aging is off by default. When on:

- Password aging affects all Linux and CMS users who use the `/usr/bin/cms` shell. However, you can exclude specific users from the password aging policy, see Excluding a user from password aging on page 126.
  - Non-CMS users such as *root*, *root2*, or *informix* do not age.
  - If you are using LDAP, the server running the directory service controls password aging.
- When password aging is on, the system modifies the RHEL policy file `/etc/passwd`.

**Important:**

- To avoid additional password administration, Avaya recommend that you exclude specific users before turning password aging on.

**Related links**

Excluding a user from password aging on page 126
Switching password aging on/off (passwd_age) on page 67
Checking user password status on page 127
Removing a user from the aging exclusion file on page 128

Setting a different password aging for a user on page 129

# Excluding a user from password aging

## About this task

You can use this procedure to exclude specific CMS or Linux users from password aging. For example, to exclude user accounts used by custom applications that link to CMS.

- To avoid additional password administration, Avaya recommend that you exclude specific users before turning password aging on.

## Before you begin

- Check the status of the user's password. See Checking user password status on page 127.

## Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Run `cd /cms/db`
3. Run `vi age_pw_exclude`
4. Add the username you want to exclude from password aging.
5. Save and close the file by pressing `Esc` and then entering **`:wq!`**
6. If password aging was previously in effect for the user, run `passwd -x -1 <username>` where **`<username>`** is the username and `1` is the number one.

### Related links

Configuring password aging on page 125

# Switching password aging on/off (passwd_age)

## About this task

Password aging is off by default. You can use this process to turn password aging on/off, and to set the default number of days for aging.

When password aging is on:

- Password aging affects all Linux and CMS users who use the `/usr/bin/cms` shell. However, you can exclude specific users from the password aging policy, see Excluding a user from password aging on page 126.
  - Non-CMS users such as *root*, *root2*, or *informix* do not age.
  - If you are using LDAP, the server running the directory service controls password aging.
- When password aging is on, the system modifies the RHEL policy file `/etc/passwd`.

**Important:**

- To avoid additional password administration, Avaya recommend that you exclude specific users before turning password aging on.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Enter **cmsadm**. The system displays the administration menu.
3. Enter the number associated with the **passwd_age** option. The output displays the following:

```
1) Turn on password aging
2) Turn off password aging
3) Change password aging interval
or q to quit: (default 1)
```

4. Do one of the following:
   - **To turn password aging on:**

     Enter `1`. CMS prompts you to also enter the number of weeks before passwords expire. You can enter a value between 1 and 52 weeks. If you do not enter a value, CMS sets the default passwords aging to 9 weeks.
   - **To turn password aging off:**

     Enter `2` and then enter `y` to confirm when prompted.
   - **To change the current default password aging period:**

     Enter `3` to change the password current password aging interval and then specify the maximum number of weeks before passwords expire. You can enter a value between 1 and 52.

### Related links

Using the CMSADM menu on page 60
Configuring password aging on page 125

# Checking user password status

### About this task

You can use this procedure to check if password aging is enabled for a particular user.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Run `passwd -S <username>` where <*username*> is the user's username.

The system displays the status of the user's password in the following format:

- `<username> <password status> <timestamp> <minimum days> <maximum days> <warning days> <inactivity> (<status message>)`

  where:

  - `<username>` is the users username.
  - `<password status>` is either `LK` (locked) or `PS` (password set).
  - `<timestamp>` is the date the last password change.
  - `<minimum days>` is the minimum number of days allowed between password changes. `0` indicates no restriction.
  - `<maximum days>` is the number of days a new password remains valid. `99999` indicates that the system is not aging the password.
  - `<warning days>` is the number of days warning in advance of a password expiring given to a user when they log in.
    - CMS does not display a password age warning to users who access CMS through Supervisor. CMS only prompts those users to enter a new password when their password has expired.
  - `<inactive>` is the number of days after password expiry after which the user account is also disabled. `-1` indicates that this feature is not used.
  - `<message>` is a summary message about the password status.

For example:

- The user has not created a password. Password aging does not start until after a user sets a password.

  ```
  user1 LK <timestamp> 0 99999 7 -1 (Password locked.)
  ```

- The user has set a password which is not aging:

  ```
  user1 PS <timestamp> 0 99999 7 -1 (Password set, SHA512 crypt.)
  ```

- The user's has set a password which is aging:

  ```
  user1 PS <timestamp> 0 14 7 -1 (Password set, SHA512 crypt.)
  ```

- The user's password is locked:

  ```
  user1 LK <timestamp> x xxxxx x xx (Password locked.)
  ```

**Related links**

Configuring password aging on page 125

# Removing a user from the aging exclusion file

## About this task

You can use this procedure to remove a user's username from the password aging exclusion file. The user's password will then start to age.

### Before you begin

- Check the status of the user's password. See Checking user password status on page 127.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Run `cd /cms/db`
3. Run `vi age_pw_exclude`
4. Remove the username of the user whose password you want to age.
5. Save and close the file by pressing `Esc` and then entering **`:wq!`**
6. Run `passwd -x <maximum days> -w 7 <username>` where:
   - <*maximum days*> is the number of days before the password expires.
   - <*username*> is the username of the user.

### Related links

Configuring password aging on page 125

## Setting a different password aging for a user

### About this task

Turning password aging on sets a default aging period for affected users (see Switching password aging on/off (passwd_age) on page 67). You can use this procedure to specify the aging period for a specific user.

### Procedure

1. Log in to the CMS server with root privileges.
   - To log in as root from a remote connection, you must log in using an CMS user ID, then enter *su - root* to log on with root privileges
2. Run `passwd -x <maximum days> -w 7 <username>` where:
   - <*maximum days*> is the number of days before the password expires.
   - <*username*> is the username of the user.

### Related links

Configuring password aging on page 125

# Maintaining the chkDisks crontab

The chkDisks crontab runs each night and checks to see whether any potential or actual drive problems have been logged. For example, loss of the primary boot drive. The results of the search are mailed to the root user.

## Verifying chkDisks

### About this task

To verify that cron is running:

### Procedure

1. Log on as root to Linux.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

2. Enter:**`crontab -l`**
3. Check the listing to see that there is an entry for chkDisks.

## Changing the chkDisks run time

The line tells the system to run chkDisks every day at 0 minutes past hour zero (12:00 AM). You can change that schedule by changing the first five fields as necessary. The fields, in order of appearance, are: minute, hour, day of the month, month of the year, and day of the week. An asterisk means “all legal values.” The /olds/chkDisks line in the cron file is generally in the following format:

```
0 * * * * /olds/chkDisks > /dev/null 2>&1
```

For more information, see the manual (man) page for the crontab command.

## Canceling chkDisks

### About this task

To stop cron from running:

### Procedure

1. Log on as root to Linux.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on sing an administered CMS user ID, then use su - root to log on with root privileges.

2. Enter: **`crontab -e`**

3. With the file loaded in the editor, comment out the entry for chkDisks and write and quit the file.

# About the Archiving process

### The System Setup:

Storage Intervals window contains the information on when archiving takes place. See the following example:

In this example, the ACD default time zone is Eastern Standard Time. The daily archiver runs at 12:35 am Eastern Standard Time each day.

Archiving for all administered time zones for all tenants and ACDs runs at this same time each day.

The weekly archive runs two hours after the daily archive on Sunday each week. Sunday is the day after the weekly stop day of Saturday.

The monthly archive runs four hours after the daily archive on the first day of each month and creates the monthly archive for the previous month.

For more information, see About time zone archiving with additional time zones on page 131

# About time zone archiving with additional time zones

For daily archive to complete, a full 24 hours of interval data must be available for the ACD time zone and any other additional time zone. If a full 24 hours of interval data is not available for a particular time zone, the daily archiver will use the next oldest relevant range of interval data for the daily archive.

For example, the archiver is administered to run at 12:35 am Eastern Standard Time (EST). If a tenant is administered with the Pacific Standard Time (PST) zone, the actual time in PST is 8:35 am the previous day when the archiver runs at 12:35 am EST. This time is 4 hours earlier and implies that the previous day is not yet complete in PST.

Therefore, when the daily archive runs at 12:35 am Eastern Standard Time on a Sunday, the full 24 hours for Saturday has not yet completed in the Pacific Standard Time Zone. The daily archive will complete for the 24 hour period of Saturday in Eastern Standard Time, but the daily archiver cannot complete archiving for the Pacific Standard Time zone since 24 hours of data does not yet exist for Saturday.

The daily archiver will use the next oldest 24 hour period for the Pacific Standard Time zone and create a daily archive for Friday. The result is that the daily archives of some time zones will lag

behind the default time zone depending on the actual time differences that exist. See the following diagram:

The weekly archiver is run the day after the administered Week Stop Day and will run two hours after the daily archive on that day.

For weekly archiving, the previous seven daily archives are used, if available, to create the weekly archive. If all seven daily archives for the previous week are not available for the given time zone, the weekly archiver uses what is available. Thus, a weekly archive can be incomplete for some time zones. See the following example:

Monthly archiving is executed on the first day of the month, four hours after the daily archive for that day. Like the daily and weekly archives, if all the daily and weekly archives from the previous month are not available, the monthly archiver uses what is available for the given time zone. Depending on the timing of the monthly archive, some monthly archives can be missing some data.

To mitigate the lag in time zones, the Data summarizing time on the System Setup: Storage Intervals window can be changed.

Using the example of Eastern Standard (EST) and Pacific Standard Time (PST), if the Data summarizing time is changed from 12:35 am to 4:35 am, the daily archiver runs at 4:35 am EST. Thus, the previous day completes in PST and the daily archive for Saturday can be created for PST.

Since this type of change in Data summarizing time delays all archiving, customers must take care not to schedule archiving during peak busy hours. In this example, when the daily archive is set to 4:35 am, the weekly archive takes place at 6:35 am and the monthly archive at 8:35 am.

# Chapter 6: Recovering a CMS server

This chapter provides the procedures for recovering data on a Call Management System (CMS) that has non-functioning hardware or software corruption.

## Back up CMS

If the server is operational, do a CMSADM backup as shown in . If the server is not operational, you must use the most recent CMS backup available for the recovery procedure.

**Important:**

If you have to use an old backup for recovery, any administrative changes made on the CMS server since the backup was made are lost and must be re-administered after you recover the system.

## Deploy a new CMS server

To recover a failed CMS virtual machine, you must redeploy a new virtual machine as described in *Deploying Avaya Call Management System*. Verify the deployment before you attempt to restore the customer data onto the new CMS virtual machine.

## Restore CMS setup using a CMSADM backup

### About this task

You can use this process to restore your CMS data from a CMSADM backup onto the new CMS server.

**Important:**

When using NFS for backups on CMS 18.0.2 or later, you must use NFS Version 4 (v4). If upgrading from an earlier version of CMS that supports an earlier version of NFS, upgrade your NFS setup to NFS v4 after you upgrade your CMS system.

### Procedure

1. To create an NFS mount point for the CMSADM backup device, enter:

   `mkdir [NFSMountPoint]`

   where:

   - `[NFSMountPoint]` is a directory to which to attach the backup file system.

   For example, enter: `mkdir /a`

2. To mount the NFS file system, enter:

   `mount [NFSServer]:[NFSDirectory] [NFSMountPoint]`

   where:

   - `[NFSServer]` is the server hosting the backup file system.
   - `[NFSDirectory]` is the directory path to the backup file system on the backup server.

3. To list the backup files on the NFS mounted folder, enter: `ls –al [NFSMountPoint]`

4. Identify the backup file required. The backup file names use the format `CMSADM-rNNxx.y-yymmddnnnnnn-host` where:

   - `CMSADM` = The type of backup.
   - `rNNxx.y` = The CMS version of the backup.
   - `yymmdd` = The date of the backup.
   - `nnnnnn` = The unique identifier of the backup.
   - `host` = The hostname of the backed up CMS server.

5. Change to the `/tmp` folder by entering `cd /tmp`

6. To copy the contents of the required backup file, enter:

   ```
   cpio -icumdv -C 10240 -I [NFSMountPoint]/[CMSADMFilename] "/cms/install/bin/restore"
   ```

   For example:

   ```
   cpio -icumdv -C 10240 -I /a/CMSADM-r2000.1-231116151708-cms1 "/cms/install/bin/restore"
   ```

7. If the backup is encrypted, you are prompted to enter the passphrase.

8. Once the backup file contents have been copied, press `Ctrl+C` to stop the system continuing to search the CMSADM backup media device.

   - If not stopped, the system will search the entire backup media device which could take several hours to complete.

9. To ensure that the restore script is executable, enter:

```
chmod +x /cms/install/bin/restore
```

- The restore will fail if the script is not made executable.

10. To restore the CMS data from the CMSAADMF file, enter:

```
/cms/install/bin/restore /[MountPoint]/[CMSADMFilename]
```

- The system restores the files from the backup media. Following the restoration, the CMS system automatically reboots.

# Restore CMS data using a CMS Maintenance restore

After you do a CMSADM restore, you must do one of the following maintenance restores:

- Use a maintenance restore as described in this procedure.

## Data restore requirements

Before you do a CMS maintenance restore, you must meet the following requirements depending on the type of data you want to restore:

| Data to be restored | System requirements |
|---|---|
| Historical and non-CMS | • The CMS software can be in a multiuser state<br>• Data collection can be on |
| Local system administration | • The CMS software must be in the single-user state<br>• Data collection must be turned off |
| ACD-specific administration | • The CMS software must be in the single-user state<br>Data collection can be on |
| CMS server administration | • The CMS software must be in the single-user state<br>Data collection can be on |

## Before restoring data

The following items should be read and understood before restoring data:

- Data must be backed up before it can be restored. To ensure the safety of your data, you should frequently back up your system.
- When migrating or restoring a non-LDAP user from a maintenance backup, and the “logid” (logon ID) for a user does not exist in /etc/passwd, the user is created as a new logid. That logid requires password administration just as if the user was created as a new user as described in the Admin guide.

When this happens, the migration and restore logs contain messages similar to the following examples:

```
- /cms/maint/r3mig/mig.log
INFO: New UNIX user normusr1: name, room and telephone will not be
migrated.
- /cms/maint/restore/rest.log
Created UNIX login 'normusr1'.
Warning: Name, Telephone, and Room will not be restored for
normusr1.
```

# Restoring data from a full maintenance backup

## About this task

**Caution:**

Do this procedure when only the full CMS maintenance backups are available. If an incremental maintenance backup is also available, see Restoring data from a full and incremental maintenance backup on page 137.

## Procedure

1. Load, install, or mount the most recent full maintenance backup media.

   **Note:**

   At this point the system will not contain any customer defined Backup/Restore Devices for USB storage devices or network mount points. If the backup media is on a USB storage device or network mount point you will need to create a Backup/Restore Device, using the CMS menu options **Maintenance | Backup/Restore Devices**, before the data can be restored. If the backup media is on a USB storage device refer to the section Administering a backup or restore device for a USB storage device on page 101. If the backup media is on a network mount point refer to the section Administering a Backup/Restore Device for a network mount point on page 115.

2. From one of the windows at a console, log in to the system by using a CMS administrator login ID, for example, `su - cms`. Enter the correct password if prompted.

3. Enter `cms`

   A series of prompts about system status may appear before the system displays the CMS main menu.

4. Enter the correct terminal type.

   - If the CMS version on the backup media is the same CMS version installed on the system then the data can be restored, continue with Step 5.
   - If the CMS version on the backup media is the not the same CMS version installed on the system then the data needs to be migrated, continue with Step 7.

5. Select the **Maintenance** option.

6. Select the **Restore Data** option. In the **Restore from last backup (y/n)** field, enter: `n`

7. Select the **System Setup** option.
8. Select the **R3 Migrate Data** option. Continue with Step 9.
9. Enter the Device name that you want to restore/migrate data from. This can be the name of the tape device, the NFS mount point or the USB storage device. You can get the device names by pressing `Enter`, selecting **List devices** and pressing `Enter` again.
10. For the remaining options, do not make any changes.
11. Press `Enter`, select **Run** and press **Enter** again.

    **Note:**

    To execute a Restore/Migrate operation, CMS has to be in single user mode and data collection for the switch has to be turned off.
12. The system restores/migrates the system administration data, ACD-specific data, historical data, and non-CMS data.

    **Note:**

    If the restore/migrate action fails, select **Maintenance** > **Error Log Report** to analyze the cause of failure.
13. Go to the Free Space Allocation window that is located in the CMS System Setup subsystem and verify that no adjustments need to be made. For more information about Free Space Allocation, see *Administering Avaya Call Management System*.

# Restoring data from a full and incremental maintenance backup

## About this task

**Caution:**

Do this procedure only if both full and incremental CMS maintenance backups are available. If only a full maintenance backup is available, see Restoring data from a full maintenance backup on page 136.

## Procedure

1. Load, install, or mount the most recent full maintenance backup media.
2. From one of the windows at a console, log in to the system by using a CMS administrator login ID. For example, su - cms. Enter the correct password if prompted.
3. Enter `cms`.

   A series of prompts about system status may appear before the system displays the CMS main menu.
4. Enter the correct terminal type.

5. Depending on the type of data to be restored, it may not be necessary to do one of the following steps. See the table in Data restore requirements on page 135 to determine which steps to do.
   - To change the CMS software to single user mode:
     a. Select **System Setup - CMS State**.

        The CMS State window is displayed.

     b. Enter an `x` in the **Single-user mode** field and press `Enter` twice.

     c. Press `F5` to return to the main menu.
   - Turn off data collection:
     a. Select **System Setup - Data Collection**.

        The Data Collection window is displayed.

     b. Enter the name of the ACD.

     c. Use `Tab` to move the Off field and enter: `x`

     d. Press `Enter`, select **Modify**, and press `Enter` again.

     e. Repeat Steps a through d for each ACD.

     f. Press `F5`.
6. Select **Maintenance - Restore Data**.
7. In the Restore Data window, select the following options:

| Item | Values specified or selected |
|---|---|
| **Device name** | Tape Device name<br>USB storage device name<br>Network Device name |
| **Restore from last backup?** | n |
| **Restore historical data from** | (leave blank) |
| **ACDs to restore** | All ACDs |
| **Data to restore** | Local System Administration data<br>ACD-specific administration data<br>Historical data<br>Non-CMS data |

8. Press `Enter`, select **Run**, and press `Enter` again.
9. When the full maintenance restore is finished:
   a. Remove the full backup media and insert the most current incremental backup media.
   b. Repeat Steps 7 and 8 as needed.

c. Continue with Step 10.

10. After the incremental restore is finished, press `F5`.

    The CMS main menu is displayed.

11. Depending on the type of data to be restored, it may not be necessary to do Steps a or b. See the table in Data restore requirements on page 135 to determine which steps to do.

    a. Turn data collection on:

        a. Select **System Setup - Data Collection**.

           The Data Collection window is displayed.

        b. Enter the name of the ACD.

        c. Use the `Tab` key to move to the **On** field and enter: `x`

        d. Press `Enter`, select **Modify**, and press `Enter` again.

        e. Repeat Steps i through iv for each ACD.

        f. Press `F5`.

           The CMS main menu is displayed.

    b. Take the CMS software out of single user mode:

        a. Select **System Setup - CMS State**.

           The CMS State window displays.

        b. Enter an `x` in the **Multi-user mode** field and press `Enter` twice.

        c. Press `F5`.

           The CMS main menu is displayed.

12. Select **Logout** and press `Enter`.

13. Go to the Free Space Allocation window that is located in the CMS System Setup subsystem and verify that no adjustments need to be made.

    For more information about Free Space Allocation, see *Administering Avaya Call Management System*.

# Restoring data using a binary backup

The binary restore procedure restores the entire database from the binary backup file. This procedure does not allow system data, call center administration data, or historical data to be restored individually.

The binary backup file is used to restore the CMS database after a CMSADM restore has been performed which means that the binary backup file and CMSADM backup must have been created with the same version of CMS.

You can restore binary data from a tape, a USB storage device, or from a network mount point.

## Restore database using a binary backup from tape

### Procedure

1. Log on to CMS as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

2. Do one of the following:
   - If a CMSADM restore was performed to recover the system due to system failures, disk crashes, or power outages, continue with Step 3.
   - If a CMSADM restore was not performed to recover the system, continue with Step 6.
3. Insert the CMSADM backup tape into the tape drive.
4. Change to the root directory:**`cd /`**
5. To restore custom reports, enter:**`cpio -imudv -C 10240 -I /dev/st0 "cms/db/gem/c_custom/*" "/cms/db/gem/h_custom/*" "cms/db/gem/r_custom/*"`**
6. Insert the binary backup tape into the tape drive.
7. To restore the database enter:**`/cms/install/bin/db_restore <tape_device>`**

   If a <tape_device> is not entered, the default device will be /dev/st0.

## Restore database using a binary backup from a mount point

### About this task

To restore a binary backup from a USB storage device or a network mount point, do the following steps:

### Procedure

1. Log on to CMS as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

2. Do one of the following:
   - If you performed a CMSADM restore to recover the system due to system failures, disk crashes, or power outages, continue with Step 3.
   - If you performed a CMSADM restore to recover the system, continue with Step 6.
3. Mount the backup device containing the CMSADM backup.
4. Change to the root directory:**`cd /`**

5. To restore custom reports, which are backed up as part of the CMSADM backup, enter the following command on a single line:**cpio -imudv -C 10240 -I {mount_point/CMSADM_filename} "cms/db/gem/c_custom/*" "cms/db/gem/h_custom/*" "cms/db/gem/r_custom/*"**

   where backup_media_path is dependent on the media type.

   Example of backup_media_paths:

| | |
|---|---|
| USB storage device | **/CMS_Backup/<CMSADM_filename>** |
| Network mount point | **/NS_backup_dir/<CMSADM_filename>** |

6. If the mount point to the binary backup file does not exist, remount the mount point and verify it is accessible.

   **Note:**

   If a mount point does not exist do one of the following steps to create the mount point:

   - If the binary backup file is on a USB storage device refer to Configuring and Connecting a USB storage device on page 98.
   - If the binary backup file is on a network server refer to Configuring and Connecting to a network mount point on page 104.

7. Run the restore script:**/cms/install/bin/db_restore /<mount_point/<binary_backup_filename>**

# Using tapeless migration

Tapeless migration is necessary when upgrading from a system that has a tape drive to a new CMS server that does not. In this case, the Remote Tape Migration (RTM) tool, which is available from downloads on the support site, is used to copy the CMS maintenance backup tape on the existing system to a file on the new system. Once this file is created, you can migrate data from that file. The use of the RTM tool is only performed once and when the migration is completed, the customer should do backups using one of the supported tapeless backup options for the new system. For more on tape and non-tape device compatibility, see section related to tape compatibility in *Upgrading Avaya Call Management System*.

# Chapter 7: Additional restore procedures

This chapter contains additional restore procedures that are used to restore CMS setup data and CMS data. Use these procedures to recover when a disk drive fails or when the software or data has become corrupt.

## Recovering a mirrored system after disk failure

This section contains procedures for the recovery of a mirrored system after disk drive failure.

**Important:**

The system will need to be rebuilt to factory standards and any data will need to be restored if both disks in a matched pair fail. If this condition is met, see Doing a CMSADM restore of a system on page 142.

### Prerequisites P195

Before you recover a mirrored system, do the following tasks:

- Verify that the alternate boot device is set up.
- Search the output for Failed or Degraded device(s).
- Identify the faulty disk or disks.
- The system must boot off of a functioning boot disk.

## Doing a CMSADM restore of a system

This section describes how to restore an entire system. You must re-enable the system to boot. Then restore the system software from the CMSADM backup tape. You will have to restore the system if a mirror pair of disks fail

## Prerequisites

Before you begin restoring the system, do the following tasks:

- Obtain the CMSADM file system backup tapes.
- Obtain the most recent maintenance backup tapes.
- Replace any defective hardware.

## Restoring a system from a CMSADM backup

### About this task

This section provides the procedures for restoring a system from a CMSADM backup.

Read the following Important message if any of the following are true:

- You have changed the motherboard of the CMS server since the last cmsadm backup was run.
- The system is a Virtual CMS.

### Procedure

1. Verify that disks are installed in slots 0, 1, 2 and 3.
2. Disconnect all USB storage devices and put them in a safe place.

   **Important:**

   Remove all USB storage devices. If any USB storage devices are connected to the system, the restore process uses the USB storage device for the boot hard drive and the system fails to boot after the restore process completes.
3. Turn on power to all the external devices, such as tape drives.
4. Turn on the monitor.

   **Important:**

   If the system prompts about a change in configuration while powering up, press `F` to accept the current configuration.
5. Power on the system.
6. Insert the Avaya RHEL KICKSTART software DVD disc into the disc drive.

   You can use BIOS settings to configure the CD or DVD-ROM as the first boot device.
7. The system should boot from the DVD and display startup messages.

   **Note:**

   If the system does not boot from the DVD you will need to reboot the system using the **`shutdown -r`** now command

   The system displays the following messages as the system boots:

```
.
.
.
Initializing Firmware Interfaces…
Initialization Complete
.
Lifecycle Controller: Collecting System Inventory…
Scanning for devices…
.
.
```

The system can display the following message: `Press any key to continue.`

8. 8. If the systems displays this message, press `Enter`.

   The system displays a list of Usage options once the system boots to the Avaya RHEL software disc.

```
########################## IMPORTANT!!
############################
##      PROCEEDING WILL INSTALL A NEW OPERATING SYSTEM.
##
##      ALL DATA WILL BE LOST!! PROCEED WITH CAUTION.
##
#################################################################
##

USAGE:
Type “ks” then press <enter> to install preconfigured Linux and
copy CMS software to the disk.
Type “rs” then press <enter> to install preconfigured Linux and
make the system ready to restore from a CMSADM backup.
Type “rescue” then press <enter> to rescue installed system

boot:
```

9. Enter `rs` at the **boot**: prompt. Press `Enter`.

   **Note:**

   The system displays blue Welcome to Red Hat Enterprise Linux for x86_64 screens as the various packages get installed.

   **Important:**

   Do not leave the system unattended before configuring the network device as this can result in the screen becoming blank. If the screen becomes blank, and the user returns and presses the Enter key to activate the screen, the system can interpret the entry as accepting eth0 as the ethernet port to configure.

10. The system displays the following messages as the Linux® operating system is installed:

```
Loadingvmlinuxz…
.
.
```

11. The system displays the NetworkingDevice screen.

    **Note:**

    Use the arrow keys to toggle between the options.

12. By default, the system selects both the IPv4 and IPv6 network options. Use the space bar to select and deselect options.

    **Important:**

    You must select the **Manual Configuration** option under the **IPv4** option.

    - If the customer is not using IPv4, clear IPv4.
    - If the customer is using IPv6, select the appropriate item from the **IPv6** options that meets the requirements of the customer.
    - If the customer is using IPv4, select **Manual Configuration** under the **IPv4** options.
    - If the customer is not using IPv6, clear IPv6.
    - If the customer is using IPv6, select the appropriate item from the IPv6 options that meets the requirements of the customer.

13. Use the right arrow key to highlight the **OK** button. Press `Enter`.

    The system displays the Manual TCP/IP Configuration screen. Use the down arrow key to move through the input fields.

| | |
|---|---|
| IPv4 Address/Netmask | 198.1.1.1/255.255.255.0 |
| Gateway | 198.1.1.254 |
| Name Server | 198.1.1.10 |

    **Note:**

    The values in the above TCP/IP Configuration box are examples only.

14. Use the down arrow key to highlight the **OK** button. Press `Enter`.

    The system completes the configuration with the options selected and installs the Linux® packages.

```
Formatting
.
.
Installation Starting
.
.
Package Installation
.
.
```

```
Packages completed xxx of xxx
.
.
```

Once the system configuration is complete, the system displays a Reboot message.

```
Complete

Congratulations, your Red Hat Enterprise Linux installation is
complete.

Please reboot to use the installed system. Note that updates may
be available to ensure the proper functioning of your system and
installation of these updates is recommended after the reboot.

Reboot
```

15. If the DVD does not automatically eject from the drive, remove the DVD from the drive before continuing.
16. Press `Enter` to reboot.

    The system reboots and displays the RHEL login screen.

    **Note:**

    If the system fails to boot and displays Hard Disk Error messages, ensure that no USB storage devices are inserted into any USB slots of the system. If the system has any USB storage devices inserted, remove the USB storage device and repeat the entire restore procedure.

    **Important:**

    The installation process reconfigures eth0 with the network information previously entered for eth2.
17. Enter the encryption passphrase if the auto-unlock feature is disabled.
18. To verify the network settings on the system do the following:
    - Open the `/etc/sysconfig/network` file using the vi editor.
    - Verify the **NETWORKING** = YES
    - Verify the **HOSTNAME** and **GATEWAY IP** addresses are correct. If **HOSTNAME** and **GATEWAY** are not correct, manually change the file while in the vi editor and save the changes.
19. If you modified the `/etc/sysconfig/network` file, reboot the system. Enter: `shutdown- r now`
20. Enter the encryption passphrase if the auto-unlock feature is disabled.
21. Verify the network settings for eth0.

    Open a virtual console window.

Test your network settings to ensure that the network settings are working properly.

22. Enter: `ifconfig eth0`
23. Enter: `ping {system on your local network}`

    Press `Control+C` to exit the ping command.

    **Note:**

    If the network does not respond, enter `ifup eth0`. If the network still does not respond, repeat this procedure and verify that the values entered are correct.

24. Install the latest RHEL RPM updates which are provided by the Avaya Technical Support organization.

    You must do this step before proceeding with CMSADM restore. After the update of the RHEL RPMs, the CMS server will reboot.

25. Run the CMS security script.

    For information to run the CMS script see, Installing the Avaya CMS security script and changing the cmssvc password on page 198 for the steps to do this task. In order to run the security script, you might have to re-mount the CMS software disc. You must do this step before proceeding with the CMSADM restore.

    **Note:**

    After the security script is run, unmount the CMS software disc before continuing.

    - If the CMSADM backup is on a network mount point, continue with step 28.
    - If the CMSADM backup is on tape, continue with step 26.
    - If the CMSADM backup is on a USB device, continue with step 27.

    The system provides the following options for accessing the CMSADM backup media:

    **Caution:**

    The CMSADM backup does not preserve mount point directories. If the default backup device is a mount point then the restore process can fail during CMS setup if the mount point path does not exist. If this occurs, create the mount point path and rerun CMS setup from a flat file. Look for the default backup device path in the **`/cms/install/cms_install/cms.install`** file for the mount point path that needs to be created. For more information, see Using the flat file on page 21 on page 30 for instructions on how to run CMS setup from a flat file.

26. To access the CMSADM backup from tape:
    a. Insert the CMSADM backup tape into the tape drive.
    b. Change to the /tmp directory. Enter: `cd /tmp`
    c. Enter the following command on a single line: `cpio -icmudv -C 10240 -I /dev/st# "cms/install/bin/restore"` where `st#` is replaced with the tape device name.

d. Press `Ctrl+C`.

The system stops searching the CMSADM backup media device.

**Note:**

If you do not press `Ctrl+C`, the system continues to search the entire backup media device. This search could take several hours to complete.

e. Verify that the restore script has the correct permissions by entering:

**chmod+x /cms/install/bin/restore**

The system sets the correct permissions to run the script. If the permissions for the script are not correct, the restore fails.

f. Restore the system from the media device. Enter:

**/cms/install/bin/restore/dev/st#**

g. Continue with step 29.

27. To access the CMSADM backup from a USB storage device:

a. Insert the CMSADM backup USB storage device.

b. Determine the device number associated with the USB storage device by following the step c to step g:

c. Enter: **fdisk -l**

The output of the fdisk command looks as follows:

```
Disk /dev/sdb: 64.7 GB, 64692944896 bytes
64 heads, 32 sectors/track, 61696 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

d. Make a note of the USB_Device_Name for the USB storage device, such as sdb.

e. Create a mount point for the USB storage device. Enter: **mkdir {mountpoint}**

```
mkdir /a
```

f. 4. Mount the USB storage device.

```
mount /dev/{USB_Device_Name} {mountpoint}
```

```
mount  /dev/sdb  /a
```

g. Verify the backup files are on the USB storage device. Enter: **ls -al /a**

h. Change to the `/tmp` directory. Enter:

**cd/tmp**

i. Enter the following command on a single line:

**cpio-icmudv -C 10240 -I /{mountpoint}/<CMSADM_filename> "/cms/install/bin/restore"**

where `CMSADM_filename` is the CMSADM system backup file of interest. The CMSADM filename must be entered exactly like the path on the media device.

```
cpio-icmudv -C 10240 -I /a/CMSADM-r19ab.t-121116151708-trex
"/cms/install/bin/restore"
```

where the name of the CMSADM backup file identifies the following:

- Type of backup: `CMSADM`
- CMS version at the time of the backup: `r19ab.t`
- Date of the backup: `121116(yymmdd)`
- Unique identifier of the backup: `151708`
- CMS host name: `trex`

j. Press `Ctrl+C`.

The system stops searching the CMSADM backup media device.

**Note:**

If you do not press `Ctrl+C`, the system continues to search the entire backup media device. This search could take several hours to complete.

k. Verify that the restore script has the correct permissions by entering:

**chmod+x /cms/install/bin/restore**

The system sets the correct permissions to run the script. If the permissions for the script are not correct, the restore fails.

The system displays the following message:

```
Warning: The CMS database needs to be initialized and the
        CMS Data needs to be manually restored from a CMS
maintenance backup.
        This requires CMS and IDS to be shutdown!!!
        Do you want to continue? (y or n) :
```

l. Enter `y`.

m. Restore the system from the media device. Enter:

**/cms/install/bin/restore/{mountpoint}/<CMSADM_filename>}**

n. Continue with Step 29.

28. To access the CMSADM backup from a NFS mount point, enter:

**mkdir{NFS_Mount_point}**

**mount{NFS server}:{NFS directory} {NFS_Mount_point}**

a. Verify the backup files are on the NFS mounted directory.

**ls-al {NFS_Mount_point}**

b. Change to the `/tmp` directory, enter: **cd/tmp**

c. Enter the following command on a single line:

**cpio-icumdv -C 10240 -I {NFS_Mount_point}/{CMSADM_filename} "/cms/install/bin/restore"**

where `CMSADM_filename` is the CMSADM system backup file of interest. The CMSADM file name must be entered exactly like the path on the media device.

```
cpio-icmudv -C 10240 -I /a/CMSADM-r19ab.t-121116151708-trex
"/cms/install/bin/restore"
```

where the name of the CMSADM backup file identifies the following:

- Type of backup: `CMSADM`
- CMS version at the time of the backup: `r19ab.t`
- Date of the backup: `121116(yymmdd)`
- Unique identifier of the backup: `151708`
- CMS host name: `trex`

d. Press `Ctrl+C`.

The system stops searching the CMSADM backup media device.

**Note:**

If you do not press `Ctrl+C`, the system continues to search the entire backup media device. This search could take several hours to complete.

e. Verify that the restore script has the correct permissions by entering:

**chmod+x /cms/install/bin/restore**

The system sets the correct permissions to run the script. If the permissions for the script are not correct, the restore fails.

f. Restore the system from the media device. Enter:

**/cms/install/bin/restore {NFS_Mount_point}/{CMSADM_filename}**

g. Continue with Step 29.

29. The system restores the files on the backup media. The system automatically reboots after all the files on the media device have been transferred.

**Note:**

If a problem occurs during the restore process, the system displays prompts indicating a problem. Follow the instructions displayed by the system.

30. Log on to the system as root.

**Important:**

You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su- root` to log on with root privileges.

31. Enter the encryption passphrase if the auto-unlock feature is disabled.

    **Important:**

    The system can reboot several times during the restore process. The reboots can occur at random intervals throughout the restore process. You may have to repeat this step several times.

32. The restore process can be monitored by opening a virtual console window and entering:

    **`tail-f /cms/install/logdir/restore/restorecms.log`**

    **Note:**

    To monitor the restore progress, you must open a virtual console window and enter this command each time the system reboots.

    When the restore process is complete, the system displays the following message at the end of `restorecms.log`:

    ```
    CMS Restore Completed Successfully
    ```

    If the CMS restore completes successfully, continue with Step 38.

33. Check the CMS authorizations to see whether or not the CMS hardware feature is authorized. Enter:

    a. `cmssvc`

    b. Enter 1 to select `auth_display`.

    The system displays the current authorization status of the CMS features and capacities.

    ```
    Capability/Capacity    Authorization

    ----------------------       ------------
                                                    WebLM/Port/
    License ID    test
                                                              CMS
    release    R19
                                                         License
    Duration    02/14/20

    forecasting    authorized
                                                    external call
    history    authorized
                                                             multi-
    tenancy    authorized

    Dual IP    authorized
    ```

```
                                                                LDAP
authentication    authorized
                                                        Maximum number
of ACDs    8
                                          Simultaneous Avaya CMS Supervisor
logins    1600
                                                Number of authorized
agents (RTU)    80000
                                             Number of authorized ODBC
connections    10
                                   Number of CLInt sessions for Avaya
internal use    100
                                        Number of CLInt sessions for non
Avaya use    100
                                                                FIPS
140-2 mode    off
Firewall    off
                                       Enhanced Access Security Gateway
(EASG)    enabled
                                                  Disk encryption auto-
unlocking    enabled
```

**Note:**

The system can display different authorizations depending on the current version of CMS and the packages you installed.

Continue with Step 35.

34. View the admin log failure messages. Enter:

    **`tail-20 /cms/install/logdir/admin.log`**

    - If the admin log contains the following messages, then the backup device mount point does not exist or is not accessible. Continue with Step 35.

      ```
      Customer CMS data successfully initialized.  <timestamp>
      system () call failed (xxxx, x)
          /cms/install/bin/compress_backup -c /<mount_point> > /dev/
      null invalid input:
      Enter the default backup device path: /<mount_point>
      (0)
      ```

    - If the admin log does not provide instructions on how to resolve the problem, then escalate through normal channels.

35. Verify that the default backup device path exists and is accessible:

    a. View the `/cms/install/cms_install/cms.install` file and note the default backup device path currently defined.

    b. Create the default backup path, if it does not exist.

    c. Mount the default backup path and verify that the mount point is accessible.

36. Complete the CMS setup by entering: **/cms/install/bin/restore database**
37. You can monitor the restore process by opening a virtual console window and entering:

    **tail -f /cms/install/logdir/restore/restorecms.log**

    When the restore process is complete, the system displays the following message at the end of `restorecms.log`:

    `CMS Restore Completed Successfully`

    If the restore fails again, escalate through normal channels.
38. After the restore has completed successfully, power the system off and back on.**shutdown -h 0**

    Wait 15-30 seconds and then press the power button to power the system back on. During the boot up process, the system can do some relabeling of the disks which is acceptable.

    The system boots and displays the RHEL Welcome screen.

    **Caution:**

    CMS does not automatically restart during the boot up process when the system is powered off using the shutdown -h 0 command or if the CMS server experiences any power failures. In either of these instances, you need to manually turn on CMS using the appropriate option from the CMSSVC menu once the system is powered back on.
39. Log on to the system as root.

    **Note:**

    At this point the root password is no longer blank.

    **Important:**

    You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use `su - root` to log on with root privileges.
40. 40. Enter the encryption passphrase if the auto-unlock feature is disabled.
41. The system can display a Removed Sound Devices screen. If the system displays this screen, do the following steps:
    a. Check the Do not ask again for these devices box.
    b. Click the **Yes** button.
42. Open a virtual console window.
43. Verify the network settings after the system has rebooted.

    **ifconfig -a | more**

    `eth0` should now be setup as the port in use, instead of `eth2`.

    **ping {system on local network}**

    If the network settings are not correct, run

**/cms/toolsbin/netconfig**

For more information, see Configuring the system network on page 192 for the use of this command.

# Restoring a system without a CMSADM or system backup

## About this task

If a CMSADM backup or system backup is not available, the system must be reinstalled with all software back to the original factory configuration.

To restore a system without a CMSADM backup or system backup:

## Procedure

1. Re-install the entire operating system according to install the RHEL operating system.
2. Configure the entire operating system according to configure the RHEL operating system.
3. Re-install CMS and supporting software as described in *Deploying Avaya Call Management System*.
4. Restore any available CMS data from the most recent CMS maintenance backup.
5. Contact the Avaya Professional Services Organization (PSO) for any previously installed customization.

# Restoring specific files from the CMSADM backup

## About this task

Sometimes only specific files on a system become corrupted. Use this procedure if only specific files need to be restored from a CMSADM backup.

To restore specific files from a CMSADM backup:

## Procedure

1. Enter:`cd /`
2. Enter the following command on a single line at the command prompt:
   - If the CMSADM backup is on a USB storage device, continue with step b.
   - If the CMSADM backup is on a network mount point, continue with step c.

   a. Enter: **cpio -icmudv -C 10240 -I /{mount_point}/ <CMSADM_filename>"full_path_name"**

where mount_point is the directory on the USB storage device containing the CMSADM backup file, CMSADM_filename is replaced with the CMSADM backup filename and full_path_name is replaced with the path of the files to be restored.

For example: **cpio -icmudv -C 10240 -I /CMS_Backup/CMSADM-r19aa.w-120717150230-digger "cms/install/cms_install/cms.install"**

b. Enter: **cpio -icmudv -C 10240 -I /NS_backup_dir/<CMSADM_filename>"full_path_name"**

where /NS_backup_dir is the network mount point path containing the CMSADM backup file, CMSADM_filename is replaced with the CMSADM backup filename and full_path_name is replaced with the path of the files to be restored.

For example: **cpio -icmudv -C 10240 -I /nfsbu/CMSADM-r19aa.w-120717150230-digger "cms/install/cms_install/cms.install"**

# Restore CMS data using a CMS Maintenance restore

After you do a CMSADM restore, you must do one of the following maintenance restores:

- Use a maintenance restore as described in this procedure.

## Data restore requirements

Before you do a CMS maintenance restore, you must meet the following requirements depending on the type of data you want to restore:

| Data to be restored | System requirements |
|---|---|
| Historical and non-CMS | • The CMS software can be in a multiuser state<br>• Data collection can be on |
| Local system administration | • The CMS software must be in the single-user state<br>• Data collection must be turned off |
| ACD-specific administration | • The CMS software must be in the single-user state<br>Data collection can be on |
| CMS server administration | • The CMS software must be in the single-user state<br>Data collection can be on |

# Restoring data from a full maintenance backup

## About this task

**Caution:**

Do this procedure when only the full CMS maintenance backups are available. If an incremental maintenance backup is also available, see Restoring data from a full and incremental maintenance backup on page 137.

## Procedure

1. Load, install, or mount the most recent full maintenance backup media.

   **Note:**

   At this point the system will not contain any customer defined Backup/Restore Devices for USB storage devices or network mount points. If the backup media is on a USB storage device or network mount point you will need to create a Backup/Restore Device, using the CMS menu options **Maintenance | Backup/Restore Devices**, before the data can be restored. If the backup media is on a USB storage device refer to the section Administering a backup or restore device for a USB storage device on page 101. If the backup media is on a network mount point refer to the section Administering a Backup/Restore Device for a network mount point on page 115.

2. From one of the windows at a console, log in to the system by using a CMS administrator login ID, for example, `su - cms`. Enter the correct password if prompted.
3. Enter `cms`

   A series of prompts about system status may appear before the system displays the CMS main menu.
4. Enter the correct terminal type.
   - If the CMS version on the backup media is the same CMS version installed on the system then the data can be restored, continue with Step 5.
   - If the CMS version on the backup media is the not the same CMS version installed on the system then the data needs to be migrated, continue with Step 7.
5. Select the **Maintenance** option.
6. Select the **Restore Data** option. In the **Restore from last backup (y/n)** field, enter: `n`
7. Select the **System Setup** option.
8. Select the **R3 Migrate Data** option. Continue with Step 9.
9. Enter the Device name that you want to restore/migrate data from. This can be the name of the tape device, the NFS mount point or the USB storage device. You can get the device names by pressing `Enter`, selecting **List devices** and pressing `Enter` again.
10. For the remaining options, do not make any changes.
11. Press `Enter`, select **Run** and press **Enter** again.

**Note:**

To execute a Restore/Migrate operation, CMS has to be in single user mode and data collection for the switch has to be turned off.

12. The system restores/migrates the system administration data, ACD-specific data, historical data, and non-CMS data.

    **Note:**

    If the restore/migrate action fails, select **Maintenance** > **Error Log Report** to analyze the cause of failure.

13. Go to the Free Space Allocation window that is located in the CMS System Setup subsystem and verify that no adjustments need to be made. For more information about Free Space Allocation, see *Administering Avaya Call Management System*.

# Restoring data from a full and incremental maintenance backup

## About this task

**Caution:**

Do this procedure only if both full and incremental CMS maintenance backups are available. If only a full maintenance backup is available, see Restoring data from a full maintenance backup on page 136.

## Procedure

1. Load, install, or mount the most recent full maintenance backup media.
2. From one of the windows at a console, log in to the system by using a CMS administrator login ID. For example, su - cms. Enter the correct password if prompted.
3. Enter `cms`.

   A series of prompts about system status may appear before the system displays the CMS main menu.
4. Enter the correct terminal type.
5. Depending on the type of data to be restored, it may not be necessary to do one of the following steps. See the table in Data restore requirements on page 135 to determine which steps to do.
   - To change the CMS software to single user mode:
     a. Select **System Setup - CMS State**.

        The CMS State window is displayed.

     b. Enter an `x` in the **Single-user mode** field and press `Enter` twice.

     c. Press `F5` to return to the main menu.

- Turn off data collection:
  a. Select **System Setup - Data Collection**.
     The Data Collection window is displayed.
  b. Enter the name of the ACD.
  c. Use `Tab` to move the Off field and enter: `x`
  d. Press `Enter`, select **Modify**, and press `Enter` again.
  e. Repeat Steps a through d for each ACD.
  f. Press `F5`.

6. Select **Maintenance - Restore Data**.
7. In the Restore Data window, select the following options:

| Item | Values specified or selected |
|---|---|
| **Device name** | Tape Device name<br>USB storage device name<br>Network Device name |
| **Restore from last backup?** | n |
| **Restore historical data from** | (leave blank) |
| **ACDs to restore** | All ACDs |
| **Data to restore** | Local System Administration data<br>ACD-specific administration data<br>Historical data<br>Non-CMS data |

8. Press `Enter`, select **Run**, and press `Enter` again.
9. When the full maintenance restore is finished:
   a. Remove the full backup media and insert the most current incremental backup media.
   b. Repeat Steps 7 and 8 as needed.
   c. Continue with Step 10.
10. After the incremental restore is finished, press `F5`.
    The CMS main menu is displayed.
11. Depending on the type of data to be restored, it may not be necessary to do Steps a or b. See the table in Data restore requirements on page 135 to determine which steps to do.
    a. Turn data collection on:
       a. Select **System Setup - Data Collection**.
          The Data Collection window is displayed.

b. Enter the name of the ACD.
c. Use the `Tab` key to move to the **On** field and enter: `x`
d. Press `Enter`, select **Modify**, and press `Enter` again.
e. Repeat Steps i through iv for each ACD.
f. Press `F5`.

The CMS main menu is displayed.

b. Take the CMS software out of single user mode:

a. Select **System Setup - CMS State**.

The CMS State window displays.

b. Enter an `x` in the **Multi-user mode** field and press `Enter` twice.
c. Press `F5`.

The CMS main menu is displayed.

12. Select **Logout** and press `Enter`.
13. Go to the Free Space Allocation window that is located in the CMS System Setup subsystem and verify that no adjustments need to be made.

    For more information about Free Space Allocation, see *Administering Avaya Call Management System*.

# Restoring data using a binary backup

The binary restore procedure restores the entire database from the binary backup file. This procedure does not allow system data, call center administration data, or historical data to be restored individually.

The binary backup file is used to restore the CMS database after a CMSADM restore has been performed which means that the binary backup file and CMSADM backup must have been created with the same version of CMS.

You can restore binary data from a tape, a USB storage device, or from a network mount point.

## Restore database using a binary backup from tape

### Procedure

1. Log on to CMS as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

2. Do one of the following:

   - If a CMSADM restore was performed to recover the system due to system failures, disk crashes, or power outages, continue with Step 3.

- If a CMSADM restore was not performed to recover the system, continue with Step 6.

3. Insert the CMSADM backup tape into the tape drive.
4. Change to the root directory:**cd /**
5. To restore custom reports, enter:**cpio -imudv -C 10240 -I /dev/st0 "cms/db/gem/c_custom/*" "/cms/db/gem/h_custom/*" "cms/db/gem/r_custom/*"**
6. Insert the binary backup tape into the tape drive.
7. To restore the database enter:**/cms/install/bin/db_restore <tape_device>**

   If a <tape_device> is not entered, the default device will be /dev/st0.

## Restore database using a binary backup from a mount point

### About this task

To restore a binary backup from a USB storage device or a network mount point, do the following steps:

### Procedure

1. Log on to CMS as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

2. Do one of the following:

   - If you performed a CMSADM restore to recover the system due to system failures, disk crashes, or power outages, continue with Step 3.
   - If you performed a CMSADM restore to recover the system, continue with Step 6.

3. Mount the backup device containing the CMSADM backup.
4. Change to the root directory:**cd /**
5. To restore custom reports, which are backed up as part of the CMSADM backup, enter the following command on a single line:**cpio -imudv -C 10240 -I {mount_point/CMSADM_filename} "cms/db/gem/c_custom/*" "cms/db/gem/h_custom/*" "cms/db/gem/r_custom/*"**

   where backup_media_path is dependent on the media type.

   Example of backup_media_paths:

| | |
|---|---|
| USB storage device | **/CMS_Backup/<CMSADM_filename>** |
| Network mount point | **/NS_backup_dir/<CMSADM_filename>** |

6. If the mount point to the binary backup file does not exist, remount the mount point and verify it is accessible.

**Note:**

If a mount point does not exist do one of the following steps to create the mount point:

- If the binary backup file is on a USB storage device refer to Configuring and Connecting a USB storage device on page 98.
- If the binary backup file is on a network server refer to Configuring and Connecting to a network mount point on page 104.

7. Run the restore script:**`/cms/install/bin/db_restore /<mount_point/<binary_backup_filename>`**

## Using tapeless migration

Tapeless migration is necessary when upgrading from a system that has a tape drive to a new CMS server that does not. In this case, the Remote Tape Migration (RTM) tool, which is available from downloads on the support site, is used to copy the CMS maintenance backup tape on the existing system to a file on the new system. Once this file is created, you can migrate data from that file. The use of the RTM tool is only performed once and when the migration is completed, the customer should do backups using one of the supported tapeless backup options for the new system. For more on tape and non-tape device compatibility, see section related to tape compatibility in *Upgrading Avaya Call Management System*.

# Chapter 8: Troubleshooting

This chapter provides solutions for common software or hardware problems. Use this information to troubleshoot CMS.

## Determining your CMS version

### About this task

To determine the version of CMS installed on your system:

### Procedure

Enter: **`rpm -qa cms`**

The system displays the CMS version.

## Recognizing new hardware devices

### About this task

Use this procedure if externally powered devices, such as disk drives and tape drives, are not recognized during a RHEL installation. This problem might occur if:

- The devices are not connected to power
- The devices are not turned on
- If you add a new port board to the computer as part of an upgrade or addition

If you discover that a hardware device is not being recognized try rebooting the system. If the hardware device is still not being recognized try rebooting from the software disc and reinstalling RHEL.

### Procedure

1. Reboot the system by entering: **`shutdown -r now`**

   The system reboots.
2. Log on as root.

**Important:**

You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

3. Enter the encryption passphrase if the auto-unlock feature is disabled.

# Tracking changes to password aging

The admin log keeps a record of any administrative changes made to password aging. The system updates the admin log when the aging interval is changed or if password aging is turned on or off. The admin log can be found at **`/cms/install/logdir/admin.log`**

## Tracking changes to password aging

The admin log keeps a record of any administrative changes made to password aging. The system updates the admin log when the aging interval is changed or if password aging is turned on or off. The admin log can be found at: **`/cms/install/logdir/admin.log`**

## Passwords of excluded users age

### About this task

If a user was added to the password aging exclude list and their password is continuing to age or has begun to age:

### Procedure

1. Log on as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use su - root to log on with root privileges.

2. Enter: **`passwd -x -1 user_name`**

   where **`user_name`** is the name of the user, and where **`1`** is the number one.

# CMS logs

The following is a list of CMS logs and the information they capture:

| Location | Function |
|---|---|
| /cms/ahl/log | History of network configuration changes. |
| /cms/dc/archive/arch.log | Archive history. |
| /cms/maint/backup/back.log | Backup log. |
| /cms/env/cman/cman.log | Data cache update from CMS Web supervisor to CMS PC supervisor. |
| /usr/elog/elog | Error log - elog primary log used for troubleshooting. |
| /cms/env/gem/gem_log | User accesses to gem screens. |
| /cms/dc/harchive/harch.log | Interval archive log. |
| /cms/env/lm/license.log | License usage history log. |
| /cms/env/phl/phl.log | Performance history log. |
| /cms/env/cms_mon/proc_log | CMS processes start and end history. |
| /cms/db/qlog | Informix query log. |
| /cms/migrate/r3mig.log | Customer data migration log. |
| /cms/maint/r3mig/mig.log | Data migration log for services. |
| /cms/maint/restore/rest.log | Restore log. |
| /cms/env/gem/rt_gem | Real-time gem screen access. |
| /cms/acd[1-8]/spi.err | SPI error log. |
| /cms/acd[1-8]/spi.log | Messages between CM and CMS. |
| /cms/db/journal/timetable/ttlog | Time table (scheduler) log. |
| /cms/install/logdir/admin.log | CMS configuration administration log. |
| /cms/install/logdir/install.log | Install log. |
| /cms/env/lm/odbc_sess.log | Detailed ODBC and JDBC connection information for each audit cycle. |
| /cms/db/log/admin_chg.log | Logging of all CMS administration changes from the client. Actions logged include add, modify, delete, copy, and run. |
| /cms/acd1/spi.log | Spigate logging between AADA and CMS. |
| /cms/acd1/spigate.error | Spigate logging between AADA and CMS. |

# CMS error logs

The administrative data for each error log file contains specific information about itself, including defaults, administration information, a description of the contents, and general information about how to interpret the contents of the logs.

**Important:**

For adjusting log configuration, contact Avaya services personnel.

# Audit logging of administrative actions

## About this task

CMS logs the administrative actions of Agent and Call Center administrators in the admin_chg.log file. CMS stores the admin_chg.log file in syslog format at `/cms/db/log`.

The audit log file logs Agent and Call Center administrative tasks such as Add, Modify, Delete, Copy, and Run. However, the file does not log display-only actions, such as, List all, Find, Next, or Previous.

You can use the log file to track all CMS administration operations, including the ACD administration and the user or agent changes.

Each log entry in the admin_chg.log file includes the following details:

- Date
- Time
- Server name
- Login ID
- ACD
- Screen name
- Action
- Key field name
- ID of the task

For example: A CMS administrator, whose login ID is admin1, adds a new dictionary calculation for ACD 2 called ACW_AUX_OUT2. The log file displays the log entry for this task as follows:

```
Thu Nov 10 11:57:10 2022 cmsvm87 gem 1215269 acd=2, user=admin1,
screen=Dictionary:
 Calculations, key=Calculation name, action=Add, id=ACW_AUX_OUT2
```

Use the following procedure to view the audit log file:

## Procedure

1. Log in to CMS as root.
2. To navigate to the log directory, enter the following command: **`cd /cms/db/log`**
3. To view the log file, enter the following command: **`tail -f admin_chg.log`**

# Checking installed software packages

### About this task

Use this procedure to check for previously installed software packages. The rules for specifying package names are as follows:

- You can omit the `pkgname` variable from the command. The command then lists the name, description, and version number of every software package installed on the system.
- If you list only one package name, the command lists the name, description, and version number of only that software package.
- You can list several package names separated by spaces. The command then lists the name, description, and version number of every software package you name.

  To check what software packages are installed on your system:

### Procedure

From the root prompt, enter: **`rpm -qa pkgname`**

where `pkgname` is the name of the software package you are checking for.

# Diagnosing a machine panic

### About this task

If a machine panic is detected on your system, you must call the Avaya Services (domestic) or remote (international) support personnel. Avaya Services can request that you deliver the following information:

- Crash dump from **`/var/crash/hostname/vmcore.n`**
- Namelist from **`/var/crash/hostname/unix.n`**
- Output of the **`rpm -qa`** command. For details, see the hardware installation document for your platform.
- Possibly output from the **`/var/log/messages`** file.

To gather all the files for Avaya Services, do the following procedures:

### Procedure

1. Log on as root.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **`su - root`** to log on with root privileges.

2. Enter: **`cd /var/crash/hostname`**

   The system changes to the dump directory.

3. Verify that unix.n and vmcore.n are present and match the date for the crash in question.
4. Enter: **rpm -qa > rpm_list.out**

   The system retrieves the output from the rpm -qa command.
5. Enter: **dmesg > dmesg.out**

   The system creates a dmesg.out file.
6. Enter: **cp /var/log/messages messages**

   The system copies the output from the /var/log/messages file.
7. Enter the following command on a single line at the command prompt: **tar cvf /storage/cms_crashfiles.tar unix.X vmcore.X dmesg.out rpm_list.out messages**

   where the letter **X** represents the number of the crashdump.

   The system displays a list of all of the files.
8. Log out of the system.
9. Notify Avaya Services that the file is ready for download.

# Common problems using the disc drive

Use the following procedures if you experience problems with the disc drive.

## Verifying that the system can read a disc

### Procedure

Enter:**mount**

The system displays a list of devices and file systems currently mounted. The last line displayed must show the disc drive and the disc name.

### Example

An example of **/dev/dvd** mounted on `/mnt` message is:`/dev/sr0 on /mnt type iso9660 (ro)`

## Disc drive fails to open

If the disc drive fails to open when you press the eject button, enter the following commands:

**umount /mnt**

**eject /dev/dvd**

# Removing the CMS package fails

### Condition

If you exited the system when removing a CMS package (cms or /cms.2), you might have:

- Logged in as `cmssvc`
- Switched users - `su'd` to root or root2
- Run **`cmssvc`**

### Solution

1. Log on as root or root2.

   **Important:**

   You cannot directly log on as root from a remote connection. You must log on using an administered CMS user ID, then use **`su - root`** to log on with root privileges.

2. Remove packages as instructed by the system.

# CMS installation fails

### About this task

If the CMS installation fails and the system displays the cannot add another instance of CMS message, either the CMS package was not removed or the removal was not completely successful.

To continue with the installation:

### Procedure

1. Enter: **`cd /`**
2. Enter: **`cmssvc`**
3. Select option to **Turn Avaya CMS on or off**.
4. Enter: **`cmssvc`**
5. Select the number associated with uninstall.
6. Restart the CMS installation.

# CMSADM backup problems

If you receive an error message during a backup or recovery, refer to Common error messages on page 171.

As the backup progresses, the program displays a series of dots, one dot per file, to indicate it is writing files to tape. You may have a problem if you notice one of the following:

- Dots are not displaying (wait 10 minutes or longer to make certain the software is not just copying a very large file).
- The tape is not spinning.
- The system has not displayed messages prompting you to change tapes or informing you that the backup has completed.

Do the following

- Clean the tape drive with the appropriate cleaning tape. It may be necessary to repeat this process several times.
- If the tape drive is new, clean the drive several times with the appropriate cleaning tape before use.

If you still encounter problems, call the National Customer Care Center or your product representative.

# System messages

### About this task

System messages can alert you to system problems, such as a device that is about to fail. By default, many of the messages are displayed on the system console and are stored in /var/log. To display system messages:

### Procedure

Enter **dmesg | more**

The system displays the most recent messages as shown in the following example:

```
Initializing cgroup subsys cpuset
Initializing cgroup subsys cpu
Linux version 2.6.32-279.el6.x86_64
(mockbuild@x86-008.build.bos.redhat.com) (gc c version 4.4.6 20120305
(Red Hat 4.4.6-4) (GCC) ) #1 SMP Wed Jun 13 18:24:36 ED T 2012
Command line: ro root=UUID=3b8fa701-8689-4e03-b022-869d34fbc0be
rd_NO_LUKS  KEYB OARDTYPE=pc KEYTABLE=us LANG=en_US.UTF-8 rd_NO_MD
SYSFONT=latarcyrheb-sun16 cras hkernel=auto rd_NO_LVM biosdevname=0
rd_NO_DM rhgb quiet
KERNEL supported cpus:
Intel GenuineIntel
AMD AuthenticAMD
Centaur CentaurHauls
BIOS-provided physical RAM map:
BIOS-e820: 0000000000000000 - 000000000009c000 (usable)
BIOS-e820: 0000000000100000 - 00000000cd2f0000 (usable)
BIOS-e820: 00000000cd2f0000 - 00000000cd31c000 (reserved)
```

```
BIOS-e820: 00000000cd31c000 - 00000000cd35b000 (ACPI data)
BIOS-e820: 00000000cd35b000 - 00000000d0000000 (reserved)
BIOS-e820: 00000000e0000000 - 00000000f0000000 (reserved)
BIOS-e820: 00000000fe000000 - 0000000100000000 (reserved)
BIOS-e820: 0000000100000000 - 0000000230000000 (usable)
DMI 2.7 present.
SMBIOS version 2.7 @ 0xFD050
```

The /var/log directory contains several message files. The most recent messages are in /var/log/messages. Previous system messages are organized into weekly message files and are identified by the date that is appended to the messages file.

The message files may contain not only system messages, but also crash dumps and other data, which can cause /var/log to grow quite large. To keep the directory to a reasonable size and ensure that future crash dumps can be saved, you should remove unneeded files periodically. You can automate the task by using crontab. See your RHEL system documentation for information on crontab.

# RAID for CMS

CMS enables you to build a system with RAID 10 performance and redundancy. Having such redundancy reduces the risk of data loss should a disk drive fail or your system crash.

While RAID 10 greatly reduces the risk of losing data, it is not meant to be a substitute for regular backups. Data can still become corrupt, and the corruption is then duplicated on the mirror.

In addition, RAID 10 enables for better performance by writing data across multiple disks. CMS RAID support is enabled through an internal RAID controller.

# Troubleshooting problems with disk drives

Use the procedures and tips in this section to help you identify and resolve problems with:

- Physical disks
- RAID volumes
- `/cms` file system

Check the system console and the /var/log/messages log for messages that indicate problems with a specific hard disk.

If a disk is generating errors, it may need to be replaced.

# Common error messages

This section lists, in alphabetical order, common error messages you might encounter on a CMS server. Each message is accompanied by its probable cause and the likely solution.

- `Error in creating UNIX login for user 'username'. The user may have already had UNIX log...`

  - Cause: The user already has a Linux system login in CMS.

  - Resolution: If the user username already has a Linux system login, ignore this message. Otherwise, verify that this user can log on and report any problems to Services.

- `ERROR: Password aging cannot be implemented on systems using LDAP.`

  - Cause: The system is using LDAP.

  - Resolution: Contact your network administrator. The passwords will have to be aged from the server running the directory service.

- `Insufficient number of free blocks (#-of-blocks) in system name for temporary database tables.`

  - Cause: The file system does not contain enough free blocks for CMS to create the temporary tables needed for the migration.

  - Resolution: Call services to resolve this situation.

- `*** INTERNAL ERROR: contact services (error#, timestamp) ***`

  - Cause: An internal error occurred during processing of the table listed above this message.

  - Resolution: Contact services immediately. Do not remove the log file. Services needs the errornum and time stamp to find more information in their error log.

- `Request failed. See /cms/install/logdir/backup.log for more information.`

  - Cause: The tape is improperly seated in the drive, or was removed from the drive during the backup, or is write protected, or the medium is corrupted.

  - Resolution: Check the console terminal. If you see a message like `WARNING: ST01: HA 0 TC 3 LU 0: Err 60503005 CMD 0000000A Sense Key 00000004 Ext Sense 00000000`, the tape is corrupted. Discard it and replace it with a new tape. Otherwise, remove the tape from the drive and make sure it is not write protected (the black arrow in the upper left corner should be pointing away from “safe”).

    Finally, reinsert the tape into the drive, making certain it is properly seated, and restart the backup.

- `UNRECOVERABLE ERROR READING TAPE, errno= Failed to open tape: no entry in the device directory. Make sure the Maintenance: Backup/Restore Devices screen has the correct Path.`

  - Cause: The program could not open the tape drive to read the CMS data.

- Resolution: Check that the specified tape drive is set up with the correct path in the Maintenance: Backup/Restore Devices window. If you cannot resolve this problem, contact services for additional help. You may have a tape drive hardware problem or need a corrected tape device path.

- `** WARNING:** Only one user may run age_pw at one time.`

  - Cause: More than one person is attempting to use the passwd_age option in the CMSADM menu.

  - Resolution: Attempt to run the command after a few minutes have passed. If you still receive the warning message, contact Avaya services.

- `You must be root in order to run this command.`

  - Cause: Superuser privileges are necessary to run this script because most of the commands are related to system administration.

  - Resolution: Log in as the root user and rerun the command.

- `stale databases`

  - Cause: The state database contains old information.

  - Resolution: Recreate the database.

- `syntax error`

  - Cause: The syntax and usage of the command may be incorrect.

  - Resolution: Reenter the command, correcting syntax errors you have made.

- `The /cms filesystem needs to be mounted`

  - Cause: /cms must be mounted for the command to work.

  - Resolution: Mount /cms with the command:

    **`mount /cms`**

- `touch: /cms/db/unix_start cannot create`

  - Cause: A CMSADM backup was done when CMS was still running. An attempt is made to restart CMS, but CMS files are not yet available.

  - Resolution: No response required. The message will disappear after you have restored and migrated CMS.

- `Warning: inode blocks/cyl group (230 >= data blocks (135) in lost cylinder group. This implies 2160 sector(s) cannot be allocated.`

  - Resolution: Some sectors will not be used by the filesystem. This is just a warning; the filesystem should be fine.

- `logtime[xxx]: Failed to list SAVECORE dir contents. ERROR 0`

  - Resolution: No action required, this is an informational message only indicating that no coredump files currently exist.

# Troubleshooting reports

## Report Query Status

Two types of report query logs are being added with release R16.2. These logs track the queries made by historical reports and they show the queries that have completed and the queries that are currently being run. This information can be used to determine who is running what reports and if those report queries are affecting system performance.

### Information about query logs

- Types of report query logs:

  - qlog: a log where entries are made upon query completion

  - idbm log: a log showing the query that is currently running

- These logs are always in operation implying that they do not need to be turned off/on
- Comparison between the report query logs

  - qlog has more detail, but is only updated after the report query has completed

  - idbm log shows currently running queries and is updated at completion of the query to add completion status

- Uses of report query logs

  - qlog can show past report execution to determine who ran queries and how long the queries took

  - idbm log can be used to determine what queries are running currently. This can be used to determine if a particular query is taking a long time and thus negatively impacting system performance.

  - Log information in either logs cannot be used to kill a particular report; it is debug information only

- qlog features

  - Entries are made upon query/report completion

  - Applies to historical report queries only

  - Log entries have information about start time, user, run time, completion status, task ID and query text

  - qlogs are store in directory **`/cms/db/log as qlog, qlog.01, qlog.02,`** etc.

  - The size and number of qlog files are administered in the file **`/cms/db/LogAdmin/qlog`** on the server

  - Example entry:

```
vdn, starttime, intrvl, acdcalls, acdtime, abncalls,
busycalls,disccalls,incalls,othercalls from hvdn where row_date = 40432 and acd =
1 order by vdn, starttime
```

- idbm log features

  - Entries are made for currently running queries.

- Applies to historical report queries only.

- IDBM stands for Informix Database Manager. These are the processes that interface with the historical database.

- log entries contain information about start time, user and query text.

- The idbm logs are kept in the server in directory **/cms/db/log** as idbm.'process ID'. For example: **idbm.17, idbm.1001, idbm.13027**, etc.

- Example entry:

```
<timestamp> dsb123 select value, item_name from synonyms where item_type='split'
and acd_no=1
```

- If no query is running in that idbm process, the log will show the last query run along with its status.

- Example status entry:

```
<timestamp> STATUS=0
```

## Information about query logs

- Types of report query logs:

  - qlog: a log where entries are made upon query completion

  - idbm log: a log showing the query that is currently running

- These logs are always in operation implying that they do not need to be turned off/on

- Comparison between the report query logs

  - qlog has more detail, but is only updated after the report query has completed

  - idbm log shows currently running queries and is updated at completion of the query to add completion status

- Uses of report query logs

  - qlog can show past report execution to determine who ran queries and how long the queries took

  - idbm log can be used to determine what queries are running currently. This can be used to determine if a particular query is taking a long time and thus negatively impacting system performance.

  - Log information in either logs cannot be used to kill a particular report; it is debug information only

- qlog features

  - Entries are made upon query/report completion

  - Applies to historical report queries only

  - Log entries have information about start time, user, run time, completion status, task ID and query text

  - qlogs are store in directory /cms/db/log as qlog, qlog.01, qlog.02, etc.

- The size and number of qlog files are administered in the file /cms/db/LogAdmin/qlog on the server

- Example entry:

**vdn, starttime, intrvl, acdcalls, acdtime, abncalls, busycalls,disccalls,incalls,othercalls from hvdn where row_date = 40432 and acd = 1 order by vdn, starttime**

- idbm log features

- Entries are made for currently running queries.

- Applies to historical report queries only.

- IDBM stands for Informix Database Manager. These are the processes that interface with the historical database.

- log entries contain information about start time, user and query text.

- The idbm logs are kept in the server in directory /cms/db/log as idbm.'process ID'. For example: idbm.17, idbm.1001, idbm.13027, etc.

- Example entry:

**<timestamp> dsb123 select value, item_name from synonyms where item_type='split' and acd_no=1**

- If no query is running in that idbm process, the log will show the last query run along with its status.

- Example status entry:

**<timestamp> STATUS=0**

# Report database updates

CMS R21.0.1 and later versions include a Database Change Log feature that tracks and logs all database updates initiated by a logged-in CMS user. The log is in the form of a list of each database QUERY along with date and time.

For example, `Fri Oct 11 08:46:27 2024 USER=cmssvc TIME=00:00 STATUS=0 TASK=17 QUERY= update vectors set (rd,wrt,exception) = ( "y","n","n" ) where acd=1 and ((vector = 100)) and uid in (select uid from users where l_name="username" )`

Only successful updates are logged. This log helps identify who made a database update and when.

This log is complementary to the `qlog` (Query log) which logs read access to the database.

# Location and configuration of the updatelog

The size and quantity of update log files administered is located in `/cms/db/LogAdmin`. The "updatelog" file specifies the log file location, rollover size, and the number of rollover files.

Data can be lost if log files roll over past the archive limit. The update log files will be stored in `/cms/db/log` in the form of updatelog, updatelog.01, updatelog.02, etc.

## Troubleshooting an empty or incomplete report

### Procedure

1. Check the user permissions:
   - Does the user have permission to view the skills, trunks, VDNs, and other entities they are trying to use as report input?
   - Have proper permissions been granted to the user for the resources or tenant access?
   - Are the missing resources like agent, VDN, and skills assigned to the tenant?
2. Check the time zone archiving Information
   - Does the tenant have a time zone administered?

     **Note:**

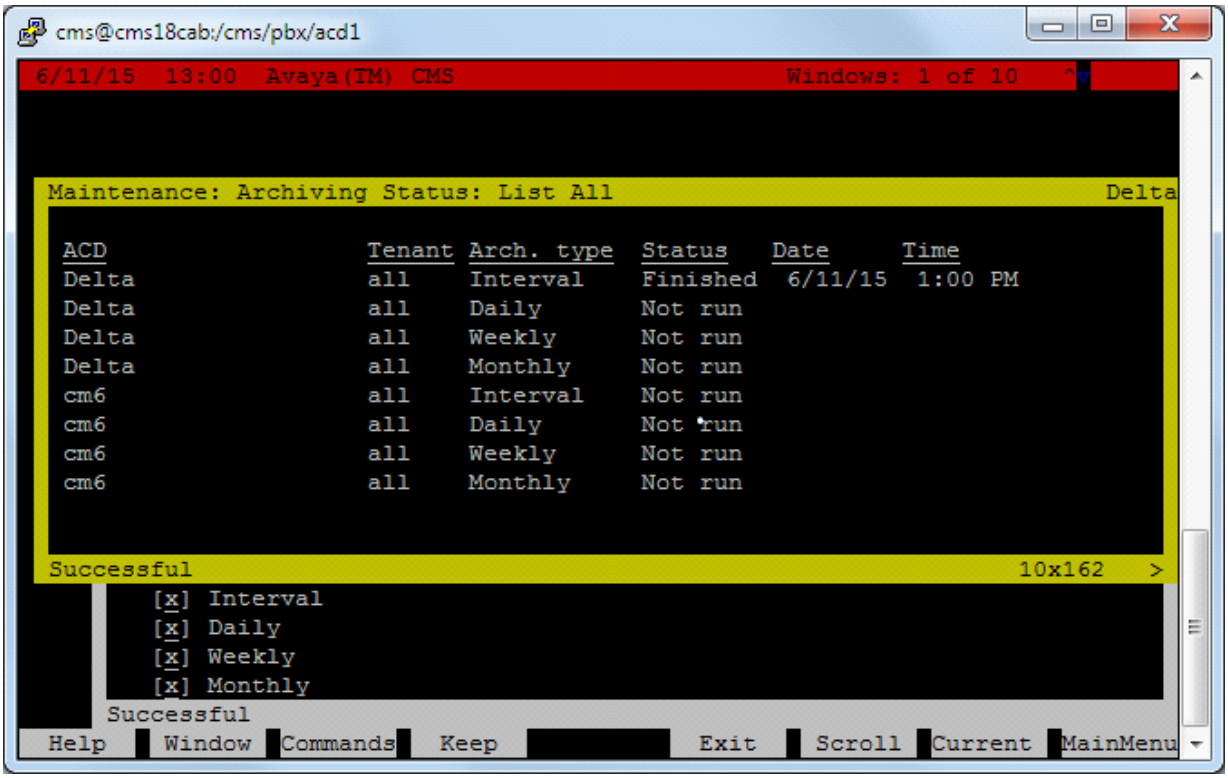
     If you do not administer the time zone, the archiver will not run for that time zone. No daily, weekly, or monthly data will be available for the time zone.
   - Has the archive run for the desired time zone?
3. For detailed debugging information, see About the Archiving process on page 131. If the archive data is not available, the report is empty for daily, weekly and monthly data.

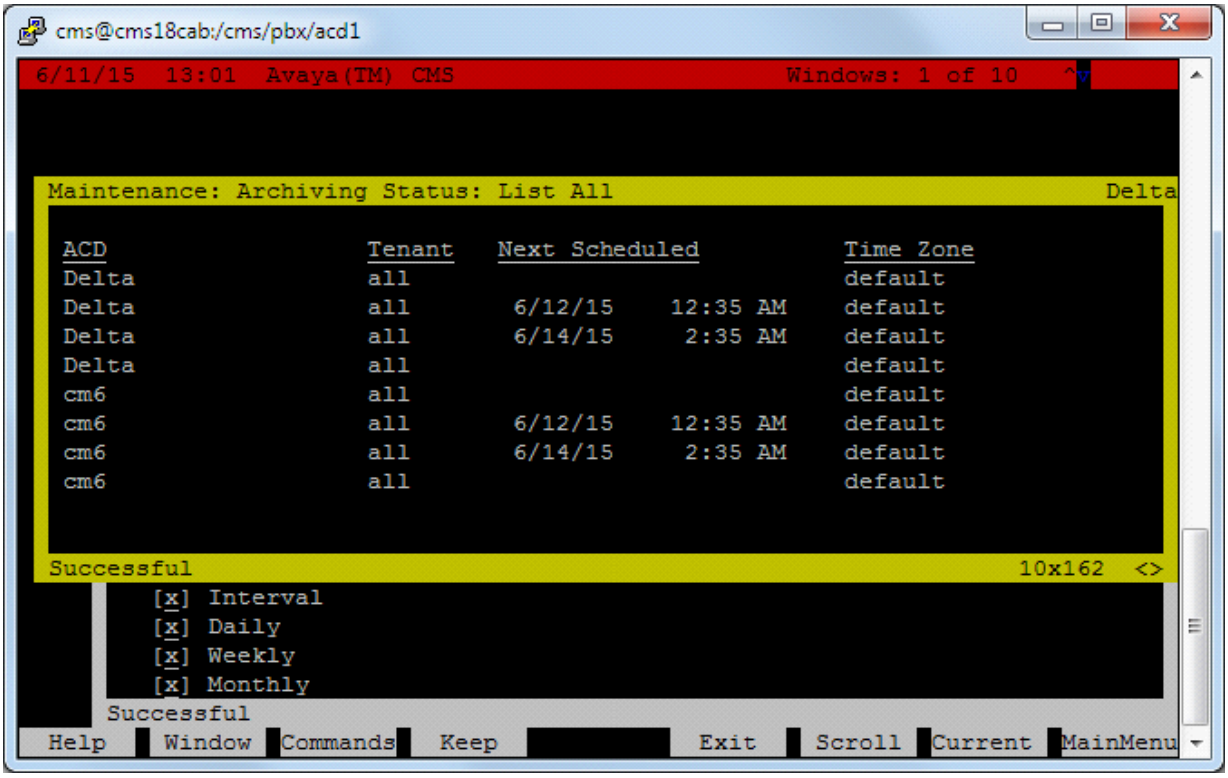
## Troubleshooting Workmode status icon on Integrated Reports

When an agent logs out, the Workmode status icon appears as '?' in the web report. The workaround for this is to add an extra column to the query that is used for IDs and icons, and for synonyms use the original column.

# How to determine whether the archiver has run

The Maintenance:Archiving Status report gives a summary of recent archive activity for the ACD and administered tenants. In the following examples, the daily archives have not yet run for ACD “Delta” and ACD “cm6”.



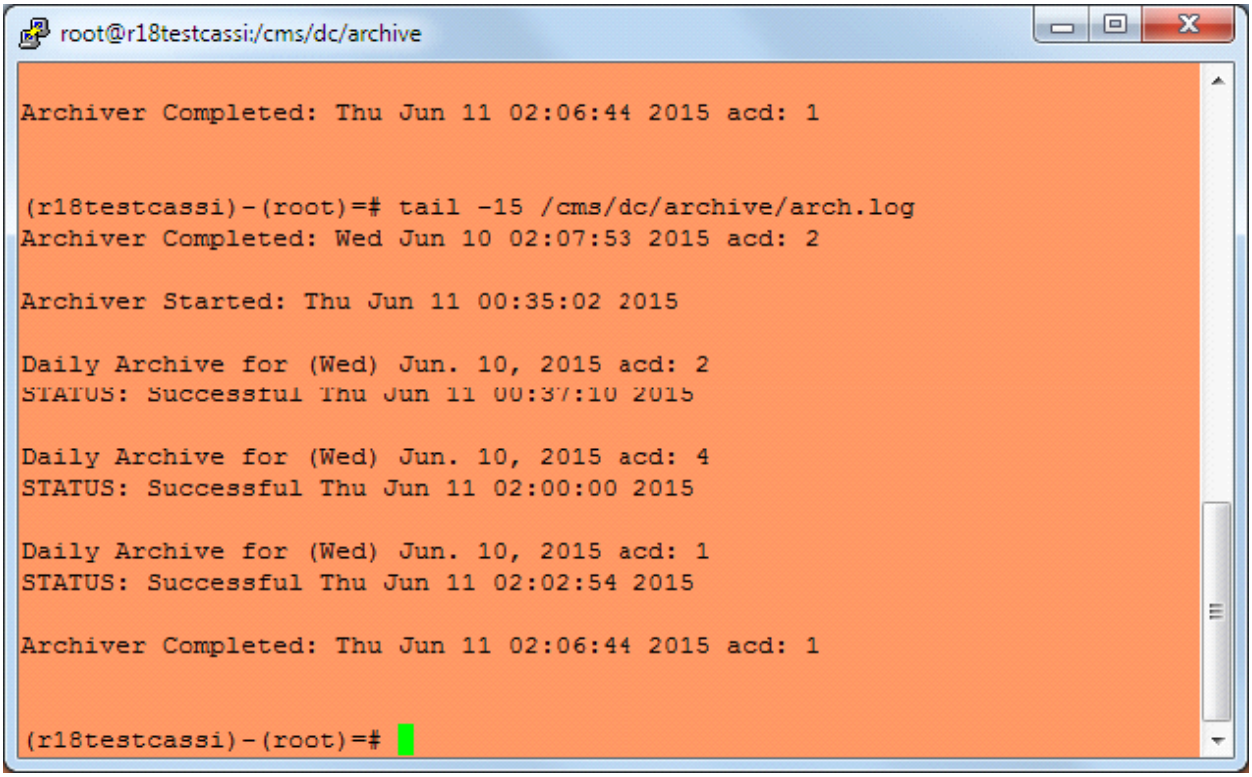




Messages are also stored in the arch.log file that provides details on archive execution. The arch.log file indicates successful archive activity and provides details about failed archive

execution. If the Maintenance:Archiving Status report indicates failure, you can view arch.log for further details. See the following example:

```
Archiver Started: Mon Jun 15 07:01:04 2015
Weekly Archive (input date: (Sun) Jun. 14, 2015) Cannot archive a partial weeks data.
STATUS: Failure Mon Jun 15 07:03:04 2015
Archiver Completed: Mon Jun 15 07:05:08 2015 acd: 1
```

The following is an example of successful arch.log entries:




Even if the archiver runs successfully, you might not see data in the report. You can verify that the actual rows of data exist for the time zone and date range input to the report by running an SQL query.

For example, the following SQL statement can show you if the time zone archive data is in the dsplit table: `select acd, row_date, split, tenant, timezone from dsplit where row_date="06/10/15"`

# Troubleshooting Visual Basic Errors

### About this task

The following table describes some of the Visual Basic errors seen while running CMS Supervisor:

## About this task

| Error Code | Error Message |
|---|---|
| 3 | Return without GoSub |
| 5 | Invalid procedure call |
| 6 | Overflow |
| 7 | Out of memory |
| 9 | Subscript out of range |
| 10 | This array is fixed or temporarily locked |
| 11 | Division by zero |
| 13 | Type mismatch |
| 14 | Out of string space |
| 16 | Expression too complex |
| 17 | Cannot perform requested operation |
| 18 | Resume without error |
| 20 | Resume without error |
| 28 | Out of stack space |
| 35 | Sub, function, or property not defined |
| 47 | Too many DLL application clients |
| 48 | Error in loading DLL |
| 49 | Bad DLL calling convention |
| 51 | Internal error |
| 52 | Bad file name or number |
| 53 | File not found |
| 54 | Bad file mode |
| 55 | File already open |
| 57 | Device I/O error |
| 58 | File already exists |
| 59 | Bad record length |
| 61 | Disk full |
| 62 | Input past end of line |
| 63 | Bad record number |
| 67 | Too many files |
| 68 | Device unavailable |
| 70 | Permission denied |
| 71 | Disk not ready |
| 74 | Cannot rename with different drive |

*Table continues…*

| Error Code | Error Message |
|---|---|
| 75 | Path/File access error |
| 76 | Path not found |
| 91 | Object variable or With block variable not set |
| 92 | For Loop not initialized |
| 93 | Invalid pattern string |
| 94 | Invalid use of Null |
| 298 | System DLL could not be loaded |
| 320 | Cannot use character device names in specified file names |
| 321 | Invalid file format |
| 322 | Cannot create necessary temporary file |
| 325 | Invalid format in resource file |
| 327 | Data value named was not found |
| 328 | Illegal parameter; cannot write arrays |
| 335 | Could not access system registry |
| 336 | ActiveX component not correctly registered |
| 337 | ActiveX component not found |
| 338 | ActiveX component did not correctly run |
| 360 | Object already loaded |
| 361 | Cannot load or unload this object |
| 363 | Specified ActiveX control not found |
| 364 | Object was unloaded |
| 365 | Unable to unload within this context |
| 368 | The specified file is out of date. This program requires a newer version |
| 371 | The specified object cannot be used as an owner form for Show |
| 380 | Invalid property value |
| 381 | Invalid property-array index |
| 382 | Property Set cannot be executed at run time |
| 383 | Property Set cannot be used with a read-only property |
| 385 | Need property-array index |
| 387 | Property Set not permitted |
| 393 | Property Get cannot be executed at run time |

*Table continues…*

| Error Code | Error Message |
|---|---|
| 394 | Property Get cannot be executed on write-only property |
| 400 | Form already displayed; cannot show modally |
| 402 | Code must close topmost modal form first |
| 419 | Permission to use object denied |
| 422 | Property not found |
| 423 | Property or method not found |
| 424 | Object required |
| 425 | Invalid object use |
| 429 | ActiveX component cannot create object or return reference to this object |
| 430 | Class does not support OLE Automation |
| 430 | Class does not support Automation |
| 432 | File name or class name not found during Automation operation |
| 438 | Object does not support this property or method |
| 440 | OLE Automation error |
| 440 | Automation error |
| 442 | Connection to type library or object library for remote process has been lost |
| 443 | Automation object does not have a default value |
| 445 | Object does not support this action |
| 446 | Object does not support named arguments |
| 447 | Object does not support current locale settings |
| 448 | Named argument not found |
| 449 | Argument not optional or invalid property assignment |
| 450 | Wrong number of arguments or invalid property assignment |
| 451 | Object not a collection |
| 452 | Invalid ordinal |
| 453 | Specified DLL function not found |
| 454 | Code resource not found |
| 455 | Code resource lock error |
| 457 | This key is already associated with an element of this collection |
| 458 | Variable uses a type not supported in Visual Basic |

*Table continues…*

| Error Code | Error Message |
|---|---|
| 459 | This component does not support events |
| 460 | Invalid Cipboard format |
| 461 | Specified format does not match format of data |
| 480 | Cannot create AutoRedraw image |
| 481 | Invalid picture |
| 482 | Printer error |
| 483 | Printer driver does not support specified property |
| 484 | Problem getting printer information from the system. Is printer is set up correctly? |
| 485 | Invalid picture type |
| 486 | Cannot print form image to this type of printer |
| 735 | Cannot save file to Temp directory |
| 744 | Search text not found |
| 746 | Replacements too long |
| 31001 | Out of memory |
| 31004 | No object |
| 31018 | Class is not set |
| 31027 | Unable to activate object |
| 31032 | Unable to create embedded object |
| 31036 | Error saving to file |
| 31037 | Error loading from file |

### About this task

You can try out the following steps towards resolving these errors:

### Procedure

1. Log out and log in back again.
2. If the error is still there, reboot the PC on which the VB error is occurring.
3. Find out if the error is occurring on any other PC on which CMS Supervisor is installed.
4. If the error is occurring on only one PC, reinstall CMS Supervisor.
5. If the error still does not go away, contact Avaya Global Support Services.

# Troubleshooting LDAP server configuration issues

This section describes the possible error messages and solutions for the LDAP server configuration. These errors can be encountered during LDAP package installation, updating LDAP configuration, or verifying the connectivity to the LDAP server.

## LDAP server log files

You can view the LDAP server logs using one of the following options:

- Search this log file for high level logs (start/complete LDAP executions). Search for “LDAP”.

  **/cms/install/logdir/admin.log**

- Search this log file for detailed logs and troubleshooting. Search for “LDAP”.

  **/cms/install/logdir/security/cms_sec.log**

## Verifying LDAP server connectivity on a non-encrypted connection

### About this task

The LDAP server connectivity test verifies the LDAP server and base distinguished name access.

### Procedure

To verify and test the connectivity of the LDAP server, use the following command: **/cms/toolsbin/ldap_connection_test**

If successful, the system displays a message similar to the following example: `LDAP Server connectivity test successfully completed.`

### Next steps

If an error is encountered, use the following failure scenarios section to identify a resolution to the problem.

## Unable to connect to the LDAP server

### Condition

Unable to connect to the LDAP server. This issue may be due to incorrect IP address, FQDN, or port number of the LDAP server.

### Solution

1. Verify the LDAP server IP address or FQDN and port number.
2. Run the following command:**ping <LDAP server IP address/FQDN>**

   If the ping is unsuccessful, there is a network configuration issue. Contact your system administrator to resolve.
3. Verify and update the LDAP authentication using the procedure Updating the LDAP authentication package configuration on page 90.

4. Run the ping command again to test the connection.
5. Verify the LDAP connectivity again using the following command:**/cms/toolsbin/ldap_connection_test**

## LDAP server authentication issues

### Condition

Condition

Connection to the LDAP Server is established, but there is a LDAP authentication issue. This issue occurs when there is a discrepancy between the LDAP server Bind Distinguished Name (DN) or Bind Distinguished Name (DN) password and configured Bind Distinguished Name (DN) or Bind Distinguished Name (DN_ password).

### Solution

1. Determine the Bind DN and Bind DN password on the LDAP server.
2. Do Updating the LDAP authentication package configuration on page 90 to verify and reconfigure the Bind DN and Bind DN password:
   - Verify that the Bind DN value is set to the LDAP Server Bind DN.
   - If the Bind DN value is not set to the LDAP Server Bind DN, set the Bind DN value to the LDAP Server Bind DN.
   - Reset the Bind DN password to the Bind DN password.
3. Verify the LDAP connectivity again using the following command: **/cms/toolsbin/ldap_connection_test**

## Base Distinguished Name access issue

### Condition

Connection to the LDAP Server has been established, but there is a Base Distinguished Name (DN) access issue.

### Solution

1. Verify whether the Base DN permission issue does not exist on the LDAP server. If a permission issue exists, correct it on the LDAP server.
2. Determine the Base DN on the LDAP server.
3. Do Updating the LDAP authentication package configuration on page 90 to verify and reconfigure the Base DN:
   - Verify that the Base DN value is set to the LDAP Server Base DN.
   - If the Base DN value is not set to the LDAP Server Base DN, set the Base DN value to the LDAP Server Base DN.
4. Verify the LDAP connectivity again using the following command: **/cms/toolsbin/ldap_connection_test**

## Unknown LDAP configuration issue

### Condition

An unknown LDAP configuration issue exists.

### Solution

1. Gather the LDAP server configuration values using the worksheet in Updating the LDAP authentication package configuration Updating the LDAP authentication package configuration on page 90.
2. Do Updating the LDAP authentication package configuration on page 90 to readminister all LDAP server parameters.
3. Verify the LDAP connectivity again using the following command:**`/cms/toolsbin/ldap_connection_test`**
4. If the issue is not resolved, contact Avaya Services.

## LDAP user authentication issue

### Condition

A CMS user has been created with LDAP authentication. The user cannot log on to CMS.

### Solution

1. Verify the LDAP connectivity using the following command: **`/cms/toolsbin/ldap_connection_test`**
2. If the test fails, verify that the CMS user is configured in the **Base Distinguished Name**.
3. Verify that the user name is configured in a user or person objectClass and that the user name is in the **sAMAccountName** field.
4. Verify that the names match exactly (spelling, capitalization, no unexpected spaces, and so on.).
5. Get the password for the CMS user.
6. Verify that you can log on to CMS is using this password.
7. Consult the following log file for log on failures for the CMS user: **`/var/log/secure`**

   The error message might indicate a specific issue that must be resolved.
8. If the issue is not resolved, contact Avaya Support.

# Troubleshooting LDAP server connectivity on an encrypted connection

The LDAP installation and configuration process executes automatic verification during attribute input and verifies LDAP server connectivity after all inputs have been validated. If there is a failure during LDAP installation or configuration, view the detailed log file failure messages at the following location to determine the cause:**`/cms/install/logdir/security/cms_sec.log`**

The following sections detail probable causes and possible solutions.

## LDAP configure input error. Re-input based on failure code (255)

### Condition

Unable to connect to the LDAP server. This issue may be due to incorrect IP address, FQDN, or port number of the LDAP server.

### Solution

1. Verify the LDAP server IP address or FQDN and port number.
2. Run the following command: **ping <LDAP server IP address/FQDN>**

   If the ping is unsuccessful, there is a network configuration issue. Contact your system administrator to resolve.
3. Verify and update the LDAP authentication using the procedure Updating the LDAP authentication package configuration on page 90.
4. Run the ping command again to test the connection.
5. If you verify that the IP address or FQDN and port are correct, the issue is with the certificate. Verify that the certificate was administered properly as described in Installing an LDAP encryption certificate on page 31 on page 45.
6. Verify the LDAP connectivity again using the following command: **/cms/toolsbin/ldap_connection_test**

## LDAP configure input error. Re-input based on failure code (49)

### Condition

Connection to the LDAP Server is established, but there is a LDAP authentication issue. This issue occurs when there is a discrepancy between the LDAP server Bind Distinguished Name (DN) or Bind Distinguished Name (DN) password and configured Bind Distinguished Name (DN) or Bind Distinguished Name (DN_ password).

### Solution

1. Determine the Bind DN and Bind DN password on the LDAP server.
2. Do Updating the LDAP authentication package configuration on page 90 to verify and reconfigure the Bind DN and Bind DN password:
   - Verify that the Bind DN value is set to the LDAP Server Bind DN.
   - If the Bind DN value is not set to the LDAP Server Bind DN, set the Bind DN value to the LDAP Server Bind DN.
   - Reset the Bind DN password to the Bind DN password.
3. Verify the LDAP connectivity again using the following command: **/cms/toolsbin/ldap_connection_test**

## LDAP configure input error. Re-input based on failure code (10, 32, or 34)

### Condition

Connection to the LDAP Server has been established, but there is a Base Distinguished Name (DN) access issue.

### Solution

1. Verify whether the Base DN permission issue does not exist on the LDAP server. If a permission issue exists, correct it on the LDAP server.
2. Determine the Base DN on the LDAP server.
3. Do Updating the LDAP authentication package configuration on page 90 to verify and reconfigure the Base DN:

- - Verify that the Base DN value is set to the LDAP Server Base DN.
- - If the Base DN value is not set to the LDAP Server Base DN, set the Base DN value to the LDAP Server Base DN.

4. Verify the LDAP connectivity again using the following command: **`/cms/toolsbin/ldap_connection_test`**

# Dictionary management

To ensure optimum performance and uninterrupted service, the CMS dictionary must be kept up-to-date. The CMS PC Supervisor has a limit of 32,000 entries in the CMS dictionary.

You can verify the current number of entries using the following query:

```
select count(*) from synonyms
```

If the query exceeds 32,000, certain dictionary values, such as agent logids, skill names, and VDN names, might not be displayed on CMS PC Supervisor reports. However, the CMS Web Supervisor continues to function normally.

You can add, modify, or delete entries in the CMS dictionary using the CMS PC Supervisor or the CMS Web Supervisor.

# Chapter 9: 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: Example of a flat file

The following display shows an example of a flat file used with the procedure Configuring CMS using a flat file on page 20. The file repeats a set of questions for ACDs 1 through 8. Enter data for only the number of ACDs (Communication Manager systems) connected to your CMS server.

```
# Enter a name for this UNIX system (up to 64 characters): localhost
# Select the type of backup device you are using #    1) Tape
#    2) Other
# Enter choice (1-2):

# Default backup device paths based on device type:
# Device    Default backup path
# Tape    /dev/st0
# Other    'none'
# Enter the default backup device path:

# Enter number of ACDs being administered (1-8):

# The following information is required per ACD:
# Information for ACD 1:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD #  1) Communication Mgr 6.x
#  2) Communication Mgr 7.x #  3) Communication Mgr 8.x #  4) CM 8.1.2+
Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS
or # /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Number of splits/skills (0-Maximum):
```

```
# Maximum number of split/skill members based on switch type:
# Release(s)    Value
# Communication Mgr 6.x    100000 # Communication Mgr 7.x/Communication
Mgr 8.x 360000 # CM 8.1.2+ Secured    360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured    2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type: # Release(s)    Value
# Communication Mgr 6.x    12000
# Communication Mgr 7.x    24000 # Communication Mgr 8.x/CM 8.1.2+
Secured  30000 # Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)    Value
# Communication Mgr 6.x    6000
# Communication Mgr 7.x    12000 # Communication Mgr 8.x/CM 8.1.2+
Secured  15000 # Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1
# Communication Mgr 8.x/CM 8.1.2+ Secured    1
# Maximum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured    1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x  30000 # Communication Mgr
8.x/CM 8.1.2+ Secured    30000 # Enter number of VDNs (0-Maximum):

# Information for ACD 2:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD #    1) Communication Mgr 6.x
#    2) Communication Mgr 7.x #    3) Communication Mgr 8.x
#    4) CM 8.1.2+ Secured # Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):
```

```
# If a host name is entered, the host name must be administered in a DNS
or # /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type: #
Release(s)    Value
# Communication Mgr 6.x    100000 # Communication Mgr 7.x/Communication
Mgr 8.x 360000 # CM 8.1.2+ Secured    360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured    2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type: # Release(s)    Value
# Communication Mgr 6.x    12000
# Communication Mgr 7.x    24000 # Communication Mgr 8.x/CM 8.1.2+
Secured  30000 # Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)    Value
# Communication Mgr 6.x    6000
# Communication Mgr 7.x    12000 # Communication Mgr 8.x/CM 8.1.2+
Secured  15000 # Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1
# Communication Mgr 8.x/CM 8.1.2+ Secured    1
# Maximum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured    1999
# Number of call work codes (Minimum-Maximum):
# Maximum number of vectors based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x  30000 # Communication Mgr
8.x/CM 8.1.2+ Secured    30000 # Enter number of VDNs (0-Maximum):
```

```
# Information for ACD 3:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD #  1) Communication Mgr 6.x
#  2) Communication Mgr 7.x #  3) Communication Mgr 8.x #  4) CM 8.1.2+
Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS
or # /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type: #
Release(s)    Value
# Communication Mgr 6.x    100000 # Communication Mgr 7.x/Communication
Mgr 8.x 360000 # CM 8.1.2+ Secured    360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured    2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type: # Release(s)    Value
# Communication Mgr 6.x    12000
#    Communication Mgr 7.x    24000
# #    Communication Mgr 8.x/CM 8.1.2+ Secured Number of trunks (0-
Maximum):    30000
# #    Maximum number of unmeasured trunks: Release(s)
Value
#    Communication Mgr 6.x    6000
#    Communication Mgr 7.x    12000
#    Communication Mgr 8.x/CM 8.1.2+ Secured    15000
# Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1
# Communication Mgr 8.x/CM 8.1.2+ Secured    1
# Maximum number of call work codes based on switch type: #
```

Example of a flat file

```
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured    1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x  30000 # Communication Mgr
8.x/CM 8.1.2+ Secured    30000 # Enter number of VDNs (0-Maximum):

# Information for ACD 4:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD #  1) Communication Mgr 6.x
#  2) Communication Mgr 7.x #  3) Communication Mgr 8.x #  4) CM 8.1.2+
Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS
or # /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type: # Release(s)
Value
#    Communication Mgr 6.x/Communication Mgr 7.x    8000
#    Communication Mgr 8.x/CM 8.1.2+ Secured    8000
#    Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type: #
Release(s)    Value
# Communication Mgr 6.x    100000 # Communication Mgr 7.x/Communication
Mgr 8.x 360000 # CM 8.1.2+ Secured    360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured    2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type: # Release(s)    Value
# Communication Mgr 6.x    12000
```

```
# Communication Mgr 7.x    24000 # Communication Mgr 8.x/CM 8.1.2+
Secured  30000 # Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)    Value
# Communication Mgr 6.x    6000
# Communication Mgr 7.x    12000 # Communication Mgr 8.x/CM 8.1.2+
Secured  15000 # Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1
# Communication Mgr 8.x/CM 8.1.2+ Secured    1
# Maximum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured    1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x  30000 # Communication Mgr
8.x/CM 8.1.2+ Secured    30000 # Enter number of VDNs (0-Maximum):

# Information for ACD 5:
# Enter switch name (up to 20 characters):
# Select the model of switch for this ACD #  1) Communication Mgr 6.x
#  2) Communication Mgr 7.x #  3) Communication Mgr 8.x #  4) CM 8.1.2+
Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS
or # /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type: #
Release(s)    Value
```

Example of a flat file

```
# Communication Mgr 6.x    100000 # Communication Mgr 7.x/Communication
Mgr 8.x 360000 # CM 8.1.2+ Secured    360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured    2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type: # Release(s)    Value
# Communication Mgr 6.x    12000
# Communication Mgr 7.x    24000 # Communication Mgr 8.x/CM 8.1.2+
Secured  30000 # Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)    Value
# Communication Mgr 6.x    6000
# Communication Mgr 7.x    12000 # Communication Mgr 8.x/CM 8.1.2+
Secured  15000 # Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1
# Communication Mgr 8.x/CM 8.1.2+ Secured    1
# Maximum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured    1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x  30000 # Communication Mgr
8.x/CM 8.1.2+ Secured    30000 # Enter number of VDNs (0-Maximum):

# Information for ACD 6:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD #  1) Communication Mgr 6.x
#  2) Communication Mgr 7.x #  3) Communication Mgr 8.x #  4) CM 8.1.2+
Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):
```

```
# If a host name is entered, the host name must be administered in a DNS
or # /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type: #
Release(s)    Value
# Communication Mgr 6.x    100000 # Communication Mgr 7.x/Communication
Mgr 8.x  360000 # CM 8.1.2+ Secured    360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured    2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type:
# Release(s)    Value
# Communication Mgr 6.x    12000
# Communication Mgr 7.x    24000 # Communication Mgr 8.x/CM 8.1.2+
Secured  30000 # Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)    Value
# Communication Mgr 6.x    6000
# Communication Mgr 7.x    12000 # Communication Mgr 8.x/CM 8.1.2+
Secured  15000 # Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1
# Communication Mgr 8.x/CM 8.1.2+ Secured    1
# Maximum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured    1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x  30000 # Communication Mgr
```

```
8.x/CM 8.1.2+ Secured    30000 # Enter number of VDNs (0-Maximum):

# Information for ACD 7:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD #  1) Communication Mgr 6.x
#  2) Communication Mgr 7.x #  3) Communication Mgr 8.x #  4) CM 8.1.2+
Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS
or # /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:
# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type: #
Release(s)    Value
# Communication Mgr 6.x    100000 # Communication Mgr 7.x/Communication
Mgr 8.x 360000 # CM 8.1.2+ Secured    360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured    2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type: # Release(s)    Value
# Communication Mgr 6.x    12000
# Communication Mgr 7.x    24000 # Communication Mgr 8.x/CM 8.1.2+
Secured  30000 # Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)    Value
# Communication Mgr 6.x    6000
# Communication Mgr 7.x    12000 # Communication Mgr 8.x/CM 8.1.2+
Secured  15000 # Number of unmeasured facilities (0-Maximum):

# Minimum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1
# Communication Mgr 8.x/CM 8.1.2+ Secured    1
# Maximum number of call work codes based on switch type: #
Release(s)    Value
```

```
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured    1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    30000
# Communication Mgr 8.x/CM 8.1.2+ Secured    30000 # Enter number of
VDNs (0-Maximum):

# Information for ACD 8:
# Enter switch name (up to 20 characters):

# Select the model of switch for this ACD #  1) Communication Mgr 6.x
#  2) Communication Mgr 7.x #  3) Communication Mgr 8.x #  4) CM 8.1.2+
Secured
# Enter choice (1-4):

# Enter the local port assigned to switch (1-64):

# Enter the remote port assigned to switch (1-64):

# If a host name is entered, the host name must be administered in a DNS
or # /etc/hosts file or the link to the switch will not work.
# Enter switch host name or IP Address:

# Enter switch TCP port number (5001-5999):

# Maximum number of splits/skills based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Number of splits/skills (0-Maximum):

# Maximum number of split/skill members based on switch type: #
Release(s)    Value
# Communication Mgr 6.x    100000 # Communication Mgr 7.x/Communication
Mgr 8.x 360000 # CM 8.1.2+ Secured    360000
# Total split/skill members, summed over all splits/skills (0-Maximum):

# Maximum number of trunk groups based on switch type: # Release(s)
Value
# Communication Mgr 6.x/Communication Mgr 7.x    2000
# Communication Mgr 8.x/CM 8.1.2+ Secured    2000
# Number of trunk groups (0-Maximum):

# Maximum number of trunks based on switch type: # Release(s)    Value
# Communication Mgr 6.x    12000
# Communication Mgr 7.x    24000 # Communication Mgr 8.x/CM 8.1.2+
```

Example of a flat file

```
Secured  30000 # Number of trunks (0-Maximum):

# Maximum number of unmeasured trunks:
# Release(s)    Value
# Communication Mgr 6.x    6000
# Communication Mgr 7.x    12000 # Communication Mgr 8.x/CM 8.1.2+
Secured  15000 # Number of unmeasured facilities (0-Maximum):
# Minimum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1
# Communication Mgr 8.x/CM 8.1.2+ Secured    1
# Maximum number of call work codes based on switch type: #
Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x    1999
# Communication Mgr 8.x/CM 8.1.2+ Secured    1999
# Number of call work codes (Minimum-Maximum):

# Maximum number of vectors based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x   8000 # Communication Mgr
8.x/CM 8.1.2+ Secured    8000 # Enter number of vectors (0-Maximum):

# Maximum number of VDNs based on switch type:
# Release(s)    Value
# Communication Mgr 6.x/Communication Mgr 7.x  30000 # Communication Mgr
8.x/CM 8.1.2+ Secured    30000 # Enter number of VDNs (0-Maximum):
```

# Index

## A


About the Archiving process ..... 131
About the configuration methods ..... 15
About time zone archiving with additional time zones ..... 131
Accessing the CMSSVC menu ..... 70
ACD
    remove ..... 62
acd_create command ..... 61
acd_remove command ..... 62
Activating the CMS Supervisor Web Client software ..... 38
Activating the license for a CMS server ..... 82
add
    ACD ..... 61
    disk space ..... 119
Adding a hard disk to use as the backup datastore ..... 112
Adding a secondary IP address to an ACD ..... 37
Additional restore procedures ..... 142
Administering a backup or restore device for a USB storage device ..... 101
Administering a Backup/Restore Device for a network mount point ..... 115
administration menu ..... 61
archive execution ..... 176
ASP 130 R6
    add disk ..... 121
Assigning passwords to the default CMS login IDs ..... 14
attach
    new disk ..... 121
Audit logging of administrative actions ..... 165
auth_display command ..... 71
Avaya InSite Knowledge Base ..... 192
Avaya support website ..... 192


## B


Backing up and restoring WebLM ..... 85
Backing up CMS to a USB storage device ..... 98
backing up data ..... 94
backup
    CMSADM troubleshooting ..... 168
Backup CMS ..... 133
backup command ..... 63
backup encryption ..... 118
backups ..... 94
Base Distinguished Name access issue ..... 184
Before restoring data ..... 135


## C


Calculating data space requirements for CMS full maintenance backups ..... 97
Calculating dataspace requirements for CMSADM backups ..... 96
Canceling chkDisks ..... 130
change history ..... 9
changing
    date and time ..... 122
Changing the chkDisks run time ..... 130
Changing the time zone ..... 123
checking
    installed software package ..... 166
Checking the contents of the CMSADM backup to a network mount point ..... 116
Checking the contents of the CMSADM backup to USB ..... 103
chkDisks ..... 130
Clearing SNMP Alarms ..... 50
CMS
    initial configuration command ..... 73
    on/off ..... 66
    unistall ..... 75
CMS administration menu ..... 61
CMS patches
    installing ..... 124
    requirements ..... 123
CMS server backup ..... 118
CMS SNMP alarm information ..... 51
CMSADM
    restoring from full and incremental backup ..... 137, 157
    restoring specific files ..... 154
    troubleshooting ..... 168
CMSADM backup ..... 95
CMSADM menu
    acd_create ..... 61
    acd_remove ..... 62
    backup ..... 63
    config_pkg ..... 70
    dbaccess ..... 68
    passwd_age ..... 67, 126
    pkg_install ..... 64
    pkg_remove ..... 64
    Please try later ..... 61
    rum_cms ..... 66
    run_ids ..... 66
    run_pkg ..... 65
CMSADM menu functions ..... 60
CMSADM restore ..... 142
cmssvc menu
    auth_display ..... 71
    EASG ..... 77
    FIPS ..... 76
    firewall ..... 78
    run_cms ..... 73
    run_ids ..... 72
    security ..... 76

cmssvc menu *(continued)*
setup ... 73
swinfo ... 73
swsetup ... 74
uninstall ... 75
weblm_set ... 72
collection
delete ... 190
edit ... 190
generating PDF ... 190
sharing content ... 190
config_pkg command ... 70
Configuring a Customer ID ... 49
Configuring a mount point on a Solaris 10 NFS server ... 105
Configuring an Alarm Destination ... 43, 56
Configuring an Alarm ID ... 48, 58
Configuring an NFS server ... 105
Configuring an SNMP User ... 45
Configuring and Connecting to a network mount point ... 104
Configuring AOM ... 42
Configuring CMS interactively ... 16
Configuring CMS software ... 12
Configuring CMS using a flat file ... 20
Configuring EASG ... 40
Configuring mount point for the CMS server ... 110
Configuring mount point for the Linux NFS server ... 108
Configuring the encryption passphrase ... 87
Configuring the mount point for a VMware virtual disk ... 113
Configuring the ODBC and JDBC server software ... 23
Configuring the standard CMS options ... 15
content
publishing PDF output ... 190
searching ... 190
sharing ... 190
sort by last updated ... 190
watching for updates ... 190
create
ACD ... 61
Creating and migrating CMS users with LDAP authentication ... 35
Creating the flat file ... 20

## D

data backup ... 94
Data restore requirements ... 135, 155
database
ODBC/JDBC access ... 68
database updates ... 175
dbaccess command ... 68
Deleting phone numbers from CMS ... 86
Deploy a new server ... 133
determine if archiver has run ... 176
determining
CMS version ... 162
devices, not recognized ... 162
disc
disc *(continued)*
drive does not mount ... 167
drive fails to open ... 167
ejecting ... 167
Disc drive fails to open ... 167
disk
add ... 119
I/O problems ... 170
disk encryption ... 81
disk failure
recovery ... 142
documentation ... 188
documentation center ... 190
finding content ... 190
navigation ... 190
documentation portal ... 190
Doing a CMS maintenance backup to a USB storage device ... 103
Doing a CMSADM backup to a network mount point . 116, 117
Doing a CMSADM backup to a USB storage device ... 102

## E

EASG
alarms ... 78
on/off ... 77
Editing the /etc/hosts file ... 24
encryption ... 81
error logs ... 164
error messages ... 171
Exmaple of a flat file ... 194

## F

feature package
configure ... 70
install ... 64
on/off ... 65
remove ... 64
finding content on documentation center ... 190
FIPS command ... 76
firewall
on/off ... 78
status ... 80

## G

generating a certificate ... 39

## H

hostname ... 74

## I

IDS

IDS *(continued)*
on/off ..... 66
Information about query logs ..... 174
Informix database
attach disk ..... 121
installation fails ..... 168
installation related problems ..... 162
Installing a license file on a WebLM server ..... 83
Installing an LDAP encryption certificate ..... 31
Installing the Dual IP package ..... 30
Installing the External Call History package ..... 27
Installing the Forecasting package ..... 25
Installing the LDAP authentication package ..... 31
Installing the LDAP feature package on CMS ..... 32
Installing the Multi-tenancy package ..... 29
installing the root certificate ..... 40
ip6tables ..... 80
iptables ..... 80
IPv6 Support ..... 24

## K

KB
Support site ..... 192
KVM
add disk ..... 121

## L

LDAP ..... 90
certificate installation ..... 90
LDAP configure input error. Re-input based on failure code (255) ..... 186
LDAP configure input error. Re-input based on failure code (49) ..... 186
LDAP configure input error.Re-inout based on failure code ..... 186
LDAP server authetication issues ..... 184
LDAP server log files ..... 183
LDAP user authentication issue ..... 185
license
WebLM server address ..... 72
link transport method ..... 73
Linux platforms ..... 10
local port
display ..... 73
set ..... 74
Locating the CMS-MIB.txt file ..... 56
location and configuration ..... 175
logs ..... 163

## M

machine panics ..... 166
Maintaining the chkDisks crontab ..... 130
Maintaining WebLM licenses ..... 82
Managing alarms and error logs ..... 84
Managing LDAP authenticated users in CMS ..... 37
Managing personal data in CMS ..... 86
menu
CMSADM menu ..... 61
missing devices ..... 162
Mount point configuration on a Linux NFS server ..... 108
Mount point configuration on a VMware datastore ..... 112
Mounting a USB storage device ..... 101

## O

off
cms ..... 66
feature package ..... 65
IDS ..... 66
on
cms ..... 66
feature package ..... 65
IDS ..... 66
OVA
add disk ..... 120

## P

package
configure ..... 70
install ..... 64
on/off ..... 65
remove ..... 64
password
check status ..... 127
password aging ..... 125
disable ..... 67, 126
enable ..... 67, 126
exclude user ..... 126
include user ..... 128
password status ..... 127
per user ..... 129
Passwords of excluded users age ..... 163
patches
installing CMS ..... 124
removing CMS ..... 125
requirements for CMS ..... 123
patches, removing ..... 125
Personal data log files ..... 87
pkg_install command ..... 64
pkg_remove command ..... 64
Please try later, setup is active ..... 61
port ..... 73, 74
Powering off CMS on a virtual machine ..... 118
Prerequisites ..... 10, 12, 15, 23, 27, 42, 143
Prerequisites P195 ..... 142
purpose ..... 9

## R


RAID for CMS ..... 170
recognizing new hardware devices ..... 162
Recovering a CMS server ..... 133
recovering a system ..... 142
related documentation ..... 188
remote port
    display ..... 73
    set ..... 74
removal fails ..... 168
remove
    ACD ..... 62
    feature package ..... 64
removing
    CMS package fails ..... 168
Removing the LDAP authentication package ..... 93
report ..... 175
Report Query Status ..... 173
Restore CMS data using a CMS Maintainance restore ..... 135, 155
Restore CMS setup using a CMSADM backup ..... 133
Restore database using a binary backup from a mount point ..... 140, 160
Restore database using a binary backup from tape .. 140, 159
restoring a system ..... 143
restoring data
    disk failure ..... 142
    disk replacement ..... 142
    specific files ..... 154
    without backup ..... 154
Restoring data from a full maintainance backup ..... 136, 156
Restoring data using a binary backup ..... 139, 159
run_cms command ..... 66, 73
run_ids command ..... 66, 72
run_pkg command ..... 65


## S


searching for content ..... 190
secondary host ..... 74
security
    disk encryption ..... 81
    EASG ..... 77
    FIPS ..... 76
    firewall ..... 78
    security command ..... 76
Sending an AOM Test Alarm ..... 49, 58
Setting the Informix configuration parameters for CMS ..... 59
Setting up AOM configuration for SNMP alarming ..... 42
Setting up CMS data storage parameters ..... 12
Setting up LAN connections ..... 23
Setting up the Alarm Origination Manager ..... 41
setup command ..... 73
sharing content ..... 190
software installation
    CMS patches ..... 123
sort documents ..... 190
starting ..... 39
starting up CMS on a virtual machine ..... 119
support ..... 192
supported hardware platforms ..... 10
supported platforms and packages ..... 10
Supported software packages ..... 10
swinfo command ..... 73
switch model
    display ..... 73
    set ..... 74
switch name
    display ..... 73
    set ..... 74
swsetup command ..... 74
system
    checking date and time ..... 122
    date and time ..... 122
    messages ..... 169
    restoring without backup ..... 154


## T


To add a secondary IP address while adding a new ACD ... 38
To modify CMS data storage parameters ..... 12
Tracking changes to password aging ..... 163
troubleshooting ..... 162
    dictionary ..... 187
    no power on peripherals ..... 162
    password aging ..... 163
    recognizing new hardware ..... 162
Troubleshooting an empty or incomplete report ..... 176
Troubleshooting LDAP server configuration issues ..... 183
Troubleshooting LDAP server connectivity on an encrypted connection ..... 185
Troubleshooting Visual Basic Errors ..... 178
Troubleshooting Workmode status icon on Integrated Reports ..... 176


## U


Unable to connect to the LDAP server ..... 183
uninstall command ..... 75
Unknown LDAP configuration issue ..... 185
Unmounting a USB storage device ..... 101
updatelog ..... 175
Updating the LDAP authentication configuration ..... 90, 91
Upgrading to WebLM ..... 85
USB storage device ..... 98
user
    exclude from password aging ..... 126
    set different password aging ..... 129
Using tapeless migration ..... 141, 161
Using the CMSADM menu ..... 60
Using the CMSSVC menu ..... 70
Using the flat file ..... 21

## V

Verifying LDAP server connectivity on a non-encrypted connection ..... 183
Verifying that the system can read a disc ..... 167
Verifying the USB storage device is recognized by the CMS server ..... 99
videos ..... 192
virtual machine
add disk ..... 119
VMware
add disk ..... 120

## W

Warning message in the License Error mode ..... 85
Warning message in the License Restricted mode ..... 85
Warning messages in error mode ..... 84
watchlist ..... 190
web Client server ..... 39
web Client software ..... 39, 40
weblm_set command ..... 72
When to do a CMSADM backup ..... 95
When to do a maintenance backup ..... 96
Working with CMS patches ..... 123