# Implementing Avaya Aura® Communication Manager Messaging

Release 7.0
Issue 2
November 2016

### Notice

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

### Documentation disclaimer

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

### Link disclaimer

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

### Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

### Hosted Service

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

### Licenses

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

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

### License type(s)

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

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

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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

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

### Heritage Nortel Software

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

### Copyright

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

### Virtualization

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

### Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies 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

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

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

### Compliance with Laws

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

### Preventing Toll Fraud

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

### Avaya Toll Fraud intervention

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

### Security Vulnerabilities

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

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

### Downloading Documentation

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

### Contact Avaya Support

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

### Trademarks

# Contents

# Chapter 1: Introduction

## Purpose

This document describes the initial configuration steps for Communication Manager Messaging after you have deployed the Virtual Machine on Avaya-provided server using Solution Deployment Manager or on VMware using vSphere. This document covers the setup of the Session Initiation Protocal (SIP) switch integration between Communication Manager Messaging and Communication Manager or Session Manager.

For information about deploying Communication Manager Messaging, see *Deploying Avaya Aura® Communication Manager Messaging*.

The information in this book is intended for use by Avaya technicians, provisioning specialists, business partners, and customers.

## Document changes since last issue

| Issue | Date | Summary of changes |
|---|---|---|
| 1 | September 2015 | Initial release |
| 2 | November 2016 | Added information about configuration changes for using CAC when the Communication Manager Messaging signaling group and PSTN are in the same network region and voice mail is enabled. |

## Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

# Chapter 2: Administering Communication Manager for Communication Manager Messaging

## Overview

Integration of the Communication Manager Messaging application with Communication Manager happens through the SIP protocol. With Communication Manager Messaging Release 7.0, the Communication Manager Messaging application comes as a standalone OVA. Prior to Release 7.0, the Communication Manager Messaging application was embedded in the Communication Manager templates. Consequently, the integration is set up with Communication Manager or Session Manager running in a separate Virtual Machine.

**Important:**

Communication Manager Messaging Release 7.0 and later does not support the administration of applications with H.323 trunk groups in a direct integration. The only supported telephony integration is SIP.

### Administer SIP integration for Communication Manager Messaging

You can administer SIP integration in the following ways:

- Direct SIP integration with Communication Manager. For more information, see Administering Direct SIP switch integration.
- SIP integration through Session Manager. For more information, see Administering SIP Integration through Session Manager.

## Communication Manager installation

This chapter provides the steps that you need to perform for administering the data on the Communication Manager virtual machine. You must deploy the Communication Manager virtual machine before administering Communication Manager. For information about deploying and configuring Communication Manager, see *Deploying Avaya Aura® Communication Manager* and *Deploying Avaya Aura® applications from Avaya Aura® System Manager*.

# Administering Communication Manager for Communication Manager Messaging

## Enabling or disabling Telnet service for Communication Manager

### Procedure

1. Log in to Communication Manager System Management Interface.
2. Click **Administration** > **Sever (Maintenance)**.
3. On the left hand navigational panel, click **Security** > **Server Access**.
4. On the Server Access page, in the **SAT over Telnet (5023)** field, do one of the following:
   - Select **Enable** to enable **SAT over Telnet (5023)**.
   - Select **Disable** to disable **SAT over Telnet (5023)**.
5. Click **Submit**.

## Starting a SAT session

### Before you begin

- Ensure that you have enabled the Telnet service for Communication Manager, before you use Telnet.

  For more information, see Enabling or disabling Telnet service for Communication Manager.

### Procedure

1. Enter the IP address for Communication Manager, for example:
   - To use PuTTy configured for SSH, enter `192.152.254.201` in the **Host Name** field and `5022` in the **Port** field.
   - To use Telnet, enter `telnet 192.152.254.201 5023`.
2. Log on to the server using an appropriate user ID.
3. Suppress alarm origination.
4. Press `Enter`.

# Checking customer options for the Communication Manager server

## About this task

Use these forms to ensure that the features are appropriately set. However, you cannot use these forms to enable the features.

**Important:**

If the customer options are not set as indicated, contact Avaya to obtain a new license file with proper features. You cannot complete the installation without proper customer options. If you do not have the correct options, contact Avaya or go to http://support.avaya.com and raise a request.

## Procedure

1. At the SAT interface prompt, type `display system-parameters customer-options`.

   The system displays the OPTIONAL FEATURES screen.
2. Verify that the **Maximum Off-PBX Telephones - OPS** field is set to the appropriate value. The value in the field determines the maximum number of SIP endpoints that can be administered.
3. Go to page 2 and verify that the **Maximum Administered SIP Trunks** field is set to the appropriate value.
4. Go to page 4 and verify that the **ARS** and **ARS/AAR Partitioning** fields are set to `y`.
5. Go to page 5 and verify that the **IP Trunks** and **ISDN-PRI** fields are set to `y`.
6. Go to page 6 and verify that the **Private Networking**, **Processor Ethernet**, and **Uniform Dialing Plan** fields are set to `y`.
7. Go to page 9 and verify that the **Basic Call Setup**, **Basic Supplementary Services**, **Supplementary Services with Rerouting**, **Transfer into QSIG Voice Mail**, and **Value-Added (VALU)** fields are set to `y`.
8. Exit the command.

# Setting feature access codes for messaging

## About this task

For messaging to function, in the System Parameters Features screen, you must create two feature access codes (FACs) and set two features to use these FACs.

## Procedure

1. Go to the SAT interface prompt and type `change dialplan analysis`.

The system displays the DIAL PLAN ANALYSIS TABLE screen.

2. Create two FACs. The FACs that you use for messaging can be one or more digits.

   For example, you can specify Dialed Strings 8 and 9 as FACs, and Dialed String 1 as a DAC.

   **Note:**

   The first FAC Dialed String value is used for the Auto Alternate Routing (AAR) setting. The second FAC Dialed String value is used for the Auto Route Selection (ARS) setting.

3. Save the changes.
4. Go to the SAT interface prompt and type `change feature-access-codes`.

   The system displays the FEATURE ACCESS CODE (FAC) screen.

5. Verify that the **Auto Alternate Routing (AAR) Access Code** field is set to the first FAC Dialed String value you entered in step 2.

   If you use the example in step 2, the Feature Access Code (FAC) for Auto Alternate Routing (AAR) Access Code would be set to 8.

6. Verify that the **Auto Route Selection (ARS) - Access Code 1** field is set to the second FAC Dialed String value you entered in step 2.

   If you use the example in step 2, the Feature Access Code (FAC) for Auto Route Selection (ARS) - Access Code 1 would be set to 9.

7. Save the changes.

### Next steps

You must also create one dial access code (DAC) for later use by the trunk group. The DAC is used to create the Trunk Access Code (TAC) while creating a trunk group for messaging.

## Setting feature parameters for messaging

### Procedure

1. Go to the SAT interface prompt and type `change system-parameters features`.

   The system displays the FEATURE-RELATED SYSTEM PARAMETERS screen.

2. Verify that the **Trunk-to-Trunk Transfer** field is set to `all`.
3. Go to page 8 and verify that the following fields are set to the proper values for the installation site:

   - **QSIG/ETSI TSC Extension**
   - **MWI - Number of Digits Per Voice Mail Subscriber**
   - **Unknown Numbers Considered Internal for Audix**
   - **Maximum Length**
   - **QSIG Path Replacement Extension**

- **Path Replace While in Queue/ Vectoring**

4. Save the changes.

## Feature-Related System Parameters field descriptions

| Parameter name | Description |
|---|---|
| **QSIG/ETSI TSC Extension** | The number in this field is an unassigned extension. It is used as a Temporary Signaling Connection for configurations where this Communication Manager server is connected to other Communication Manager servers. This number must be one in your assigned block of extensions, but is unused for any other purpose. |
| **MWI - Number of Digits Per Voice Mail Subscriber** | This value represents the number of digits used in your dial plan for the extensions that use voice mail. For example, if extensions are identified with five digits in the implementation, you would set the value in this field to 5. |
| **Unknown Numbers Considered Internal for Audix** | If an extension has not been defined in Communication Manager, this option must be set to `y`. This setting indicates that the extension number is viewed as an internal connection by messaging. |
| **Maximum Length** | When the **Unknown Numbers Considered Internal for Audix** field is set to `y`, the Maximum Length field is displayed to the right.<br>This value represents the number of digits that define a number external to the contact center. Any dialed number exceeding this value is considered an external telephone number.<br>For example, if you are using four digit extensions in your dial plan, enter 4 in this field. This field cannot be left blank. |
| **QSIG Path Replacement Extension** | This number must be within your assigned block of extensions, and not used for any other purpose. This number is usually the extension before or after the QSIG/ETSI TSC extension. |
| **Path Replace While in Queue/ Vectoring** | If you use an attendant console that has queueing or vectoring, this option must be set to `y`.<br>If this option is not set to `y`, the operator does not see where the incoming call came from, or not hear the caller for approximately 10 seconds. With vector processing the call might go to dead air. |

# Administering IP Interfaces

The Communication Manager Messaging Virtual Machine communicates with the Communication Manager Virtual Machine through the Processor Ethernet (PROCR) port of the Virtual Machine.

## Defining IP interfaces for Processor Ethernet

### Procedure

1. Type `change ip-interface procr`.

   The system displays the IP Interfaces screen.

2. Type appropriate values for the fields and save the changes.

### IP interfaces field descriptions

| Field (Page1) | Description |
|---|---|
| **Type** | The default node name is PROCR. |
| **Node name** | The unique node name for the IP interface. procr is the default node name. The node name here must already be administered on the Node Names screen. |
| **IP Address** | The IP address (on the customer LAN) of the Processor Ethernet. |
| **Subnet Mask** | The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnets, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504. |
| **Enable Interface** | The Ethernet port must be enabled (y) before it can be used. The port must be disabled (n) before changes can be made to the attributes on this screen. |
| **Network Region** | The region number for this IP interface. |
| **Target socket load** | The threshold for the number of sockets used by this CLAN within the same Gatekeeper Priority as that of other IP interfaces. If the targeted number is exceeded on a CLAN, a warning alarm is generated. If the targeted percentage is exceeded on an PE interface, a procr error is generated. |
| **Allow H.323 Endpoints** | Enter y to allow H.323 endpoint connectivity on this CLAN. Enter n if you do not want H.323 endpoints to connect to this CLAN. |
| **Allow H.248 Gateways** | Enter y to allow branch gateways to connect to this CLAN. Enter n if you do not want branch gateways to connect to this CLAN. |

*Table continues…*

| Field (Page1) | Description |
|---|---|
| **Gatekeeper Priority** | This value is used on the alternate gatekeeper list. The lower the number the higher the priority. Valid values for this field are one through nine with five being the default. This field displays only if the **Allow H.323 endpoints?** field is set to y on this screen. |

| Field (Page 2) | Description |
|---|---|
| **Node Name** | The default name is `procr6`. |
| **IP Address** | The IP address in IPv6 format of the Processor Ethernet. |
| **Subnet Mask** | The subnet mask associated with the IP address for this IP interface. For more information on IP addresses and subnets, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504. |
| **Enable Interface** | Enter `y` to enable Processor Ethernet to accept IPv6 addresses. |

# Setting parameters for system coverage

## Procedure

1. At the SAT interface prompt, type `change system-parameters coverage`.

   The system displays the SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING screen.

2. Verify that the **Coverage - Caller Response Interval (seconds)** field is set to `1`.
3. Verify that the **Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls** field is set to `n`.
4. Verify that the **Keep Held SBA at Coverage Point?** field is set to `n`.
5. Verify that the **Maintain SBA At Principal?** field is set to `n`.
6. Save the changes.

# Changing private numbering

## About this task

This task is applicable only if you have set the trunk format to private.

## Procedure

1. On the SAT interface type, `change private-numbering 1`.

2. Enter values for the following fields:
    - Ext Len
    - Ext Code
    - Trk Grp(s)
    - Total Len

    For example, if an extension and trunk are of the value 90001 and 90 respectively:
    - Ext Len: 5
    - Ext Code: 9
    - Trunk Grp(s): 90
    - Total Len: 5

    For more information about Communication Manager SAT screens, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.
3. Save the changes.

# AAR and ARS digit conversion

Depending on the **Format** field setting on Page 3 of the Trunk Group screen, you must translate the ARS and AAR digit conversion tables.

## Path replacement settings

The following table lists the AAR and ARS digit conversion translation requirements based on the trunk format.

| Trunk format setting | Digit conversion |
|---|---|
| **Private** | AAR digit conversion |
| **Public** | ARS digit conversion |
| **Unknown** | AAR digit conversion or ARS digit conversion |
| **Unk-pvt** | AAR digit conversion or ARS digit conversion |

## Converting AAR and ARS digits

### Procedure

1. At the SAT interface prompt, type `change aar digit-conversion 1`.

    The system displays the AAR Digit Conversion Table window.
2. Set appropriate values in the **Net**, **Conv**, and **Req** fields.

> **Important:**
>
> You must use values for **Matching Pattern**, **Min**, **Max**, and **Del** that are appropriate for your configuration.

3. Save the changes.
4. At the SAT interface prompt, type `change ars digit-conversion 1`.
5. Repeat steps 2 and 3.

## Saving translations

### About this task

Translations refers to the process of configuring the communication server settings through the preceding procedures. When you complete the translations, you must save them.

### Procedure

At the SAT interface prompt, type `save translation`.

The system saves the translations.

# Chapter 3: Administering Direct SIP switch integration

## Direct SIP integration between Communication Manager Messaging and Communication Manager

Communication Manager Messaging allows direct SIP integration with Communication Manager. You must administer Communication Manager SAT screens and Communication Manager Messaging System Management Interface (SMI) to implement direct SIP integration between Communication Manager and Communication Manager Messaging.

For information about Communication Manager SAT screens, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

## Adding node names for SIP integration

### Procedure

1. Type `change node-names ip`.
2. In the **Name** field, type `procr` to add an entry for SIP.
3. In the **IP Address** field, type the IP address of the processor Ethernet.
4. In the **Name** field, do one of the following:
   - Type `msgserver` for IPv4 IP addresses.
   - Type `msgserver6` for IPv6 addresses.
5. In the **IP Address** field, type the IP address of the messaging server.
6. Save the changes.

# Adding a signaling group for direct SIP integration

### Procedure

1. At the SAT command prompt, type `add signaling-group n`, where *n* is the signaling group used for SIP.
2. In the **Group Type** field, change the type to `SIP`.
3. In the **Transport Method** field, type either `tls` or `tcp` as the transport method.
4. In the **Near-end Node Name** field, type `procr`.
5. In the **Near-end Listen Port** field, type `5060` for TCP transport method and `5061` for TLS transport method.
6. In the **Far-end Node Name** field, type `msgserver`.
7. In the **Far-end Listen Port** field, type `5060` for TCP transport method and `5061` for TLS transport method.
8. In the **Far-end Network Region** field, type `1`.
9. In the **Far-end Domain** field, type the SIP domain name.

   **Note:**

   Ensure that you enter the same values on the Adding signaling group screen and the Switch Link Admin webpage of the Communication Manager Messaging web interface.
10. Save the changes.

## Add Signaling Group field descriptions

| Field | Setting |
|---|---|
| **Group Type** | SIP |
| **Transport Method** | tls or tcp |
| **Near-end Node Name** | `procr` (IPv4 IP address) or `procr6` (IPv6 IP address), depending on which interface connects to Communication Manager Messaging. |
| **Far-end Node Name** | Name of the messaging server, in IPv4 or IPv6 IP address format, that is resident on the Communication Manager Messaging server. This name is the same name that appears on the Node Names screen and has the Integrated Messaging IP address. |
| **Near-end Listen Port** | 5060 (TCP) / 5061(TLS) |
| **Far-end Listen Port** | 5060 (TCP) / 5061(TLS) |

*Table continues…*

| Field | Setting |
|---|---|
| **Far-end Network Region** | 1 is usually assigned to `procr`. If this field is left blank, Communication Manager uses the network region associated with the near-end node name. |
| **IMS Enabled** | n |
| **Far-end Domain** | Name of the SIP domain. |
| **DTMF over IP** | • `rtp-payload` if **SIP INFO for DTMF** field is set to `Ignore` on the Switch Link Admin form.<br>• `out-of-band` if **SIP INFO for DTMF** field is set to `Accept` on the Switch Link Admin form. |
| **Enable Layer 3 Test** | y |
| **Direct IP-IP Audio Connections** | y |
| **IP Audio Hairpinning** | n |

**Note:**

The fields that must be left blank must not have any values entered at this time. The values are populated later in the administration process. The fields that need not be left blank can take the default value.

If a value is not specified for the **Far-end Network Region**, the system sets the default value 1.

**Note:**

If the configuration of the **Far-end Network Region** field changes, the signaling group may not function correctly for messaging.

# Adding a trunk group for direct SIP integration

## Procedure

1. At the SAT command prompt, type `add trunk-group n`, where *n* is the trunk group number.
2. In the **Group Type** field, type `SIP`.
3. In the **TAC** field, type the DAC dialed string that you entered in the dial plan analysis.
4. In the **Service Type** field, type `tie`.
5. In the **Signaling Group** field, type the signaling group number used for SIP.
6. In the **Number of Members** field, type the value supported by the signaling group.
7. Save the changes.

# Creating a hunt group for messaging

## Procedure

1. At the SAT interface prompt, type `add hunt-group nnn`, where *nnn* represents the number of a new, unused hunt group.

   This hunt group should be consistent with your country settings, and must be used only for messaging.

   The system displays the Hunt Group screen.
2. Verify that the **Group Name** field is set to `msgserver` for IPv4 IP addresses or `msgserver6` for IPv6 addresses.
3. Verify that the **Group Type** is set to `ucd-mia`.
4. Verify that the **COR** field is set to `1`.

   **Note:**

   The COR for the hunt group must not be outward restricted.
5. Go to page 2.

   **Important:**

   Set the Message Center to the value `sip-adjunct`. This value is required for other fields to display on this page.
6. Verify that the **Message Center** field is set to `sip-adjunct`.
7. Verify that the **Voice Mail Number** field is set to the default voice mail extension.
8. Set the value of the **Voice Mail Handle** field to match the first part of the regular expression you created while administering Session Manager.

   For example, if the regular expression is *cmm@domain.avaya.com*, use *cmm* for the **Voice Mail Handle** field.
9. Verify that the value of the **Routing Digits (e.g. AAR/ARS Access Code)** field matches the FAC that you specified for the **Auto Alternate Routing (AAR) Access Code** field while setting the FACs for messaging.
10. Save the changes.

## Next steps

Change private numbering on page 14.

# Changing a route pattern

## About this task

**Important:**

For direct SIP switch integration, the route pattern must point to the SIP trunk between Communication Manager and Communication Manager Messaging.

For SIP integration through Session Manager, the route pattern must point to the SIP trunk between Communication Manager and Session Manager.

## Procedure

1. At the SAT interface prompt, type `change route-pattern nnn`, where *nnn* represents the number of the new trunk group that you created while creating a trunk group for messaging. You must enter this number for messaging to function properly.

   The system displays the route-pattern screen.
2. Verify that the fields on this window are appropriate to change the route pattern.

# Change Route-Pattern field descriptions

| Field | Setting |
|---|---|
| **Pattern Name** | The route pattern name for the messaging trunk group. For example, msgserver. |
| **Grp No.** | The number of the trunk group you created while creating a trunk group for messaging. |
| **FRL** | 0 |
| **DCS/ QSIG Intw** | n |
| **IXC** | user |
| **BCC VALUE**<br>**0 1 2 3 4 W** | y y y y y n |
| **ITC** | rest |
| **Numbering Format** | The numbering format of the trunk group. |
| **LAR** | rehu |

# Changing IP network region

## Procedure

1. At the SAT prompt, type `change ip-network-region n`, where *n* represents the value in the **Far-end Network Region** field.

The system displays the IP Network Region screen.

2. Set the value of the **Authoritative Domain** field to the SIP domain name.
3. On Page 4, in the **Codec set** column, type `1`.
4. In the **AGL** column, type `ALL`.
5. Save the changes.

# Adding a coverage path for messaging

## Procedure

1. At the SAT prompt, type `add coverage path nnn`, where *nnn* represents the number of a new, unused coverage path.

   You can substitute *nnn* with next to use the first unused coverage path number. For example, if coverage paths 1 through 5 are in use, the next parameter creates coverage path 6.

   The system displays the Coverage Path screen.
2. In the **Point1** field, type **`h`***xx*, where *xx* is the hunt group you created for messaging.

   For example, h3 represents hunt group 3.
3. Save the changes.

# Changing the IP Codec Set

## Procedure

1. At the SAT prompt, type `change ip-codec-set n`, where *n* represents the value specified for the Codec Set on the IP Network Region screen.

   The system displays the IP Codec Set screen.
2. Verify that the **Audio Codec** field is set to `G.711MU`.
3. Verify that the **Silence Suppression** field is set to `n`.
4. Go to page 2, and perform one of the following:
   - If this installation is NOT using Fax, verify that the **FAX** field is set to `relay`.
   - If this installation is using Fax, verify that the **FAX** field is set to `T.38-standard`.
5. Save the changes.

# Changing AAR analysis

### Procedure

1. Enter `change aar analysis n`, where *n* represents the first digit of the messaging extension.

   The system displays the AAR DIGIT ANALYSIS TABLE screen.

2. Verify that appropriate values are set on Page 1.

   **Important:**

   You must use values that are appropriate for your configuration. A system may use *n*–digit extensions. For example, the default messaging voice mail extension number is 30000. This number varies for every site. The columns for **Total Min** and **Total Max** refer to the number of digits in the voice mail extension. If you are using a dial plan with more than five digits, you must adjust this number accordingly.

3. Save the changes.

### Next steps

Save translations on page 16.

# Communication Manager Messaging administration

## Administering the switch link for direct SIP integration

### About this task

Perform the following steps on the Communication Manager Messaging System Management Interface.

### Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the left navigation pane, click **Switch Link Admin**.
4. In the **Extension Length** field, select the appropriate length or select **Variable** for variable extensions.

   **Note:**

   The extension length must match the length assigned to the station on Communication Manager.

5. In the **SIP Domain** field, enter the domain used for Communication Manager and Communication Manager Messaging while administering direct SIP integration.
6. In the **Far-end Connections** field, select the number of **Far-end Connections** to administer.
7. In the **Connection_n** field, type the IP address, transport type, port number, and monitor interval for each connection.
8. In the **Messaging Address** field, type the **TCP port** and the **TLS port** number.
9. In the **Messaging Ports** field, type the number of call answer ports to configure.
10. In the **Switch Trunks** field, type the total number of trunks for Communication Manager.
11. Click **Show Advanced Options**.

    The system displays advanced options that you might need to administer.
12. In the **Quality of Service** field, type a value for Call Control Per Hop Behavior (PHB) and Audio PHB or accept the default values.

    The value you enter for both the fields sets the quality of service level for call control messages and audio streams respectively on networks that support this feature. The value for both the fields must be in the range 0 to 63. The value must match the corresponding number configured for the network region used by the messaging signaling group on the switch.
13. In the **UDP Port Range** field, enter a starting UDP port number for RTP.

    The end port number is calculated automatically.
14. If you have configured SRTP for messaging, in the **Media Encryption** field, select the type of Secure Real-time Transport Protocol (SRTP) encryption for messaging. To select a **Media Encryption**:

    a. In the **Media Encryption** row, click **Clear** to remove the default value **1 : None**.

    b. Select the SRTP, you have configured for messaging, from the list and click **Add**.

    **Important:**

    You must enable the SRTP feature in the change customer-options form and set the media encryption type in the change ip-codec-set form on Communication Manager.
15. To enable DTMF transport via SIP INFO method, in the **SIP INFO FOR DTMF** field, select `Accept`.

    **Important:**

    You must set the **DTMF over IP** field to `out-of-band` on the Communication Manager **SIGNALING GROUP** screen.

    **Note:**

    This field is set to Ignore. If you change it to Accept, then any digits received from rtp-payload will be ignored.
16. Click **Save**.

## Switch Link Admin field descriptions

| Field | Description |
|---|---|
| BASIC CONFIGURATION | |
| **Extension Length** | `Variable` or any number between `1` to `50`. The number must match the dial plan of the media server. |
| **Switch Integration Type** | `SIP` |
| **IP Address Version** | The IP address version used in the IP addresses of the signaling group. The system populates this field. |
| SIP SPECIFIC CONFIGURATION | |
| **Far-end Connections** | The far-end IP address, transport type, port number, and optional monitoring interval. |
| **Connection_<n>** | Number of **Far-end Connections**. |
| **Messaging Address** | The IP address and TCP and/or TLS ports of the Communication Manager Messaging server. |
| **SIP Domain** | The SIP domain name. The domain name must match the domain name of the switch. |
| **Messaging Ports** | The number of voice ports to be configured. |
| **Switch Trunks** | The number of trunks to be configured. |
| ADVANCED OPTIONS | |
| **Quality of Service** | The value of Call Control PHB (Per Hop Behavior) and Audio PHB. This value must be in the range of 0 to 63. |
| **UDP Port range** | The starting UDP port for RTP. The system calculates the end port. |
| **Media Encryption** | The type of media encryption. The media encryption must match the media encryption administered on the switch. The following are the valid entries for this field:<br>• None<br>• srtp-aescm128-hmac32<br>• srtp-aescm128-hmac80<br>• srtp-aescm256-hmac32<br>• srtp-aescm256-hmac80 |
| **Outcall Caller ID** | The phone number or the display name or both to identify the caller for calls that are originated by the message server. |

*Table continues…*

| Field | Description |
|---|---|
| | **Note:**<br>This field is optional. If you leave this field blank, the switch determines the display information. |
| **SIP INFO for DTMF** | **Yes** for enabling out-of-band DTMF. The system will ignore all digits received through rtp-payload. |
| **Media Encryption During CapNeg** | **Enabled** is the default value. If you set this field to **Disabled**, the system sets **Media Encryption** field to **None**. This field is used only if CapNeg is present in SDP. |
| **Supported Header includes "replaces"** | `No` is the default value. This field is used to include replaces in the SIP Supported headers. |
| **Telephone Event Payload Type** | Select the RTP payload type for RFC2388 DTMF Events. This field is disabled if the **SIP INFO for DTMF** field is set to Accept. |
| **Monitor Far-end OPTIONS Messages** | Select whether messaging will monitor the far-end for SIP OPTIONS messages. If set to yes, enter the interval value (in seconds) in the **Proactive Interval** field. A value of 0 means no monitoring will be done. |
| **Inactive Link Actions** | If far-end OPTIONS monitoring is enabled, choose an action to perform if messaging does not receive a SIP OPTIONS method within the Proactive Interval timeout. |
| **Minimum Session Refresh Interval** | The minimum session refresh interval in seconds.<br>Usually, the refresh interval value is set to match the interval value administered for the switch. |
| **SIP REFER Delay** | The delay of the transfer operation in milliseconds when a Messaging outbound call is answered and the SIP REFER request sent.<br>The value range is between 0 to 5000 milliseconds. |
| **Enable Basic Transfer** | The option to enable and disable the Basic Transfer feature. If you select this check box, Messaging performs a blind transfer operation and does not directly call the destination endpoint. The gateway of the Messaging network establishes the call and transfers the two endpoints. Because the gateway establishes the call, the caller ID might change.<br>**Note:**<br>If you enable the Basic Transfer feature, Messaging does not support SIP UUI. |
| **Connection Audits** | Enable the audit of the incoming, the outgoing, and the MWI SIP connections. |

*Table continues…*

| Field | Description |
|---|---|
|  | By default, the system disconnects the connections that are idle for 30 minutes. |

## Restarting the Communication Manager Messaging application

### Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the left navigation pane, under **Utilities**, click **Stop Messaging**.

   The system displays the Stop Messaging Software page.

   The shutdown is delayed until all calls are completed. The system will end all calls that remain three minutes after beginning shutdown.
4. Click **Stop**.

   The system displays a message to indicate that Messaging is stopped.
5. After the application stops, click **Start Messaging**.

### Next steps

Complete the steps in the *Testing Communication Manager Messaging* section.

# Chapter 4: Administering SIP Integration through Session Manager

## Communication Manager Messaging SIP Integration through Session Manager

While administering SIP for Communication Manager Messaging, a trunk is not needed between Communication Manager and Communication Manager Messaging. However, a trunk needs to be created between Communication Manager and Session Manager because SIP signaling happens through Session Manager. SIP integration provides the ability to support SIP endpoints on Session Manager.

Administer Session Manager from the System Manager Web interface. Administer Communication Manager from the SAT interface. Administer Communication Manager Messaging from the SMI Web interface.

It is assumed that any endpoint that is part of this administration is registered to Communication Manager. You can have Communication Manager either as a Feature server or as an Evolution server.

Communication Manager as a Feature server only supports IP Multimedia Subsystem (IMS)-SIP users, which are registered to Session Manager. The feature server is connected to Session Manager through a SIP signalling group, which is IMS enabled. IMS enabled indicates that the feature server supports the half call model for the calls and features of the IMS users. In brief, a half call model is that in which Communication Manager communicates with Session Manager for placing calls from one IMS user to another one.

Communication Manager Evolution Server supports all types of endpoints except IMS users. It is connected to Session Manager through a signaling group, where IMS is not enabled.

**Important:**

Depending on the role Communication Manager is assigned: Feature or Evolution, you need to follow the appropriate procedures in this section.

**Note:**

While creating a trunk or link with Session manager you must use the Session Manager Asset IP address.

For detailed information about Session Manager administration field descriptions, see *Administering Avaya Aura® Session Manager*.

# Log in to the System Manager

### Procedure

1. On the web browser, enter the System Manager URL `https://<Fully Qualified Domain Name>/SMGR`.
2. In the **User ID** field, type the user name.
3. In the **Password** field, type the password.
4. Click **Log On**.

### Result

The system validates the user name and password with the System Manager user account.

- If the user name and password match, the system displays the System Manager home page with the System Manager <version_number>.
- If the user name and password does not match, System Manager displays an error message and prompts you to enter the user name and password again.

# Creating domains

### Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Domains**.
2. Click **New**.
3. In the **Name** field, enter the domain or sub-domain name.
4. In the **Type** field, select **sip** as the domain type from the drop-down menu.
5. In the **Notes** field, enter a description or other note as appropriate.
6. Click **Commit**.

# Creating Locations

### Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Locations**.
2. Click **New**.
3. In the **Name** field, enter the location name.
4. Enter notes about the location as appropriate.

5. In the Dial Plan Transparency in Survivable Mode section, enter the DPT parameters.
6. In the Overall Managed Bandwidth section, specify the parameters for the location.
7. In the Per-Call Bandwidth Parameters section, specify the average bandwidth per call for the location.
8. In the Alarm Threshold section, specify the alarm threshold percentage for audio and multimedia calls for the location.
9. To add a location pattern:
    a. Click **Add** under **Location Pattern**.
    b. Enter an IP address pattern to match.
    c. Enter notes about the location pattern as appropriate.
    d. Continue clicking the **Add** button until you have configured all the required Location Pattern matching patterns.
10. Click **Commit**.

# Create SIP entities

## SIP entity overview

SIP entities are elements that define each entity. You require entities that need to be linked. Session Manager uses the entity links to establish call flow between SIP endpoints and Communication Manager.

For SIP integration, you must:

- Create a SIP entity for Communication Manager Messaging
- Create a SIP entity for Communication Manager Feature Server or Create a SIP entity for Communication Manager Evolution Server

❗ **Important:**

You may have either Communication Manager Feature Server or Communication Manager Evolution Server.

Follow the appropriate procedure depending on the type of Communication Manager.

## Creating SIP Entities

### Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.

2. Click **New**.
3. In the General window, do the following:
   a. In the **Name** field, type the name of the SIP entity.
   b. In the **FQDN or IP Address** field, type the FQDN or IP address of the SIP entity.
   c. In the **Type** field, click Session Manager as the type of SIP entity.
   d. In the **Notes** field, type information about the SIP entity.
   e. In the **Location** field, click a location.
   f. In **Outbound Proxy**, click a proxy. For Session Manager, you must specify an Outbound Proxy.
   g. In the **Time Zone** field, click the default time zone for the SIP entity.
   h. In the **Credential name** field, type a regular expression string.

      For example: To use `www.sipentity.domain.com`, type the string `www \.sipentity\.domain\.com`.
4. For a non-Session Manager SIP Entity type, click the appropriate mode in **Loop Detection Mode**.

   The default value of **Loop Detection Mode** is **On**.
5. In the **SIP Link Monitoring** field, click one of the following:
   - **Use Session Manager Configuration**
   - **Link Monitoring Enabled**
     - In the **Proactive Monitoring Interval (in seconds)** field, type the time. The range is 1 to 9000 seconds, and the default value is 900.
     - In the **Reactive Monitoring Interval (in seconds)** field, type the time. The range is 1 to 900 seconds, and the default value is 120.
     - In the **Number of Tries** field, type a number. The range is 0 to 15, and the default value is 1.
   - **Link Monitoring Disabled**
6. To specify the Entity Links:
   a. Click **Add**.
   b. In the **Name** field, type the name.
   c. In the **SIP Entity 1** field, click the required **Session Manager** SIP Entity.

      **SIP Entity 1** must always be a Session Manager instance.
   d. In the **Protocol** field, click the appropriate protocol.
   e. In the **Port** field, type the required port.
   f. In the **SIP Entity 2** field, click the required non-Session Manager SIP Entity.
   g. In the **Port** field, type the required port.

This is the port on which you have configured the remote entity to receive requests for the specified transport protocol.

h. In the **Connection Policy** field, click the appropriate policy.

Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.

i. Click **Deny New Service** to deny service for the associated entity link.

7. **(Optional)** In the **Failover** field, add ports if the SIP entity is a failover group member.

   This step is applicable only for Session Manager SIP entity type.

8. To specify the Port parameters:

   a. Click **Add** in the Port section.

   b. Enter the necessary port and protocol parameters.

   c. To remove an incorrectly added Port, click the respective **Port** and click **Remove**.

9. For OPTIONS requests, in the **Response Code & Reason Phrase** field, add or remove a SIP code and phrase to mark the SIP entity as up or down, respectively.

10. Click **Commit**.

# Create Entity Links

## Entity Links

Routing entity links connect two SIP entities through the Session Manager to define the network topology for SIP routing.

- Entity Links connect two SIP entities.
- Trusted Hosts are indicated by assigning the **Trust State** to the link that connects the entities.

Session Manager uses an Entity Link to send or receive messages directly from the entity. You must configure an entity link between Session Manager and any administered SIP entity.

To communicate with other SIP entities in the network, each Session Manager instance must identify the port and transport protocol of the entity link to the SIP entities. The Session Manager listens on the local port for connections from the remote entity using the given transport protocol. If the **Override Port & Transport** check box is selected for the SIP entity, Session Manager uses DNS information to determine the port and transport information to the remote entity. If the **Override Port & Transport** check box is not selected for the SIP entity, Session Manager determines the port and transport information to the remote entity using the data administered in the Entity Link table.

### Deny new service state

When in the deny new service state, Entity Links do not accept new incoming calls and Session Manager does not route outgoing calls over these links. Link monitoring continues over these links but no alarms are generated for the denied links.

When placing an Entity Link into the Deny New Service state, you can:

- Take selected SIP Entities out of service for upgrades and repair without receiving numerous SIP Monitoring alarms.
- Test alternate routing paths by denying the primary link Session Manager uses on a given route.
- Deny selected links during a planned WAN outage.

You must create entity links between:

- Communication Manager Messaging and Session Manager
- Communication Manager Feature Server and Session Manager or Communication Manager Evolution Server and Session Manager

## Creating Entity Links

### Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Entity Links**.
2. Click **New**.
3. Type the name in the **Name** field.
4. Enter the SIP entity 1 by selecting the required **Session Manager** SIP entity from the drop-down list and provide the required port.

   SIP entity 1 must always be a Session Manager instance.

   The default port for TCP and UDP is 5060. The default port for TLS is 5061.
5. Enter the SIP entity 2 by selecting the required non-Session Manager SIP entity from the drop-down list and provide the required port.

   The port is the port on which you have configured the remote entity to receive requests for the specified transport protocol.
6. From the **Connection Policy** drop-down menu, select **Trusted**.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
7. Click **Commit**.

# Creating Time Ranges

### Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Time Ranges**.
2. Click **New**.
3. Enter the name, then select the required days by entering the start and end times and notes for the new time range. Start times start with the first second of the hour:minute. End Times go through the last second of the end hour:minute.
4. Click **Commit**.

# Create routing policies

## Routing policy overview

You need to create routing policies for Communication Manager and Communication Manager Messaging. A routing policy defines the destination SIP entity, time of day patterns, associates existing dial patterns and regular expressions.

While creating routing policies for Communication Manager Messaging, set Communication Manager Messaging as the SIP element destination. Similarly, while creating routing policies for Communication Manager, set Communication Manager as the SIP element destination.

## Creating Routing Policies

### Procedure

1. On the System Manager Web Console, under **Elements**, click **Routing** > **Routing Policies**.
2. Click **New**.
3. Under the General section, type a routing policy name and notes in the relevant fields.
4. In the **Retries** field, type the number of retries for the destination SIP entity.

   ✱ **Note:**

   The default value in **Retries** field is zero. The valid values are 0-5.
5. Select the **Disabled** check box to disable the routing policy.
6. Under the **SIP Entity as Destination** section, click **Select** to select the destination SIP entity for this routing policy.
7. Select the required destination and click **Select**.

8. Under the **Time of Day** section, click **Add** to associate the Time of Day routing parameters with this Routing Policy.
9. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.

   If there are gaps in the selected Time of Day coverage pattern, Session Manager displays a warning message. If such gaps exist in the Time of the Day coverage, randomness in routing selections may be observed.
10. Type the relative rankings that you want to associate with each Time Range. Lower ranking values indicate higher priority.
11. Under the Dial Patterns and Regular Expressions sections, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy.
12. Select a dial pattern from the pattern list or a regular expression from the regular expression list, and click **Select**.

    **Note:**

    This field can be left blank. The routing policy can be added to the dial pattern or regular expression when you add it.
13. Click **Commit**.

# Create dial patterns

## Dial pattern overview

Determine the dial pattern you want to use for Session Manager. Ensure that there is not conflict between the patterns you create for Communication Manager and Communication Manager Messaging.

You need to create dial patterns for:

- Communication Manager
- Communication Manager Messaging

### Considerations while creating the dial pattern for Communication Manager Messaging

- While adding dial pattern information, ensure that the dial pattern number and hunt group number match. For example, if the hunt group number is 85000, the dial pattern number must be 85000.
- Destination address must be the IP address of Communication Manager Messaging.
- Enter the dial pattern.
- Enter the minimum length of extension.

- Enter the maximum length of extension.
- Enter the SIP domain.
- Enter the **Originating Locations and Routing Policies** field to `All`.

### Considerations while creating the dial pattern for Communication Manager

- Enter the dial pattern.
- Destination address must be the IP address of Communication Manager.
- Enter the minimum extension length.
- Enter the maximum extension length.
- Enter the SIP domain.
- Enter the **Originating Locations and Routing Policies** field to `All`.

## Creating Dial Patterns

Use the Dial Patterns page to create Dial Patterns and to associate the Dial Patterns to a Routing Policy and Locations.

**Note:**

You cannot save a dial pattern unless you add at least a routing policy or a denied location.

### Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Dial Patterns**.
2. Click **New**.
3. Enter the Dial Pattern General information in the General section.

   **Note:**

   You can provide a Domain to restrict the Dial Pattern to the specified Domain.
4. Under the Originating Locations and Routing Policies section, click **Add**.
5. Select all the required Locations and Routing Policies that you want to associate with the Dial Pattern.
6. When you have finished making your selections, click **Select**.
7. To deny calls from the specified locations:
   a. Click **Add** under the Denied Locations section.
   b. Select all the Locations that are to be denied.
   c. When you have finished making your selections, click **Select**.
8. Click **Commit**.

# Regular expression for Communication Manager Messaging

The regular expression format must be expression@domain, for example cmmsip@ccdsv.com. The Communication Manager Messaging routing policy must be selected while creating the regular expression.

# Creating Regular Expressions

Use the Regular Expressions screen to create regular expressions and associate them with routing policies. You cannot save a regular expression unless the regular expression has a routing policy associated with the regular expression.

### Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Regular Expressions**.
2. Click **New**.
3. Enter the regular expression pattern in the **Pattern** field.
4. Specify a rank order for the regular expression. A lower rank order indicates a higher priority.
5. To deny routing for a matched regular expression pattern, select the **Deny** check box.
6. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
7. Select the required routing policies that you want associated with the Regular Expression by selecting the respective check boxes.
8. Click **Select** to indicate that you have completed your selections.
9. To remove an associated routing policy, select the routing policy and click **Remove**.
10. Click **Commit**.

# Communication Manager administration

## Overview

You do not need to create a trunk between Communication Manager and Communication Manager Messaging while administering SIP for Communication Manager Messaging. But, you need to create a trunk between Communication Manager and Session Manager because SIP signaling happens through Session Manager.

### Prerequisites

- Configure Communication Manager.
- Set the maximum administered SIP trunks:
    1. Log in as `init`
    2. On page 2 of the change system-parameters customer-options page set the **Maximum Administered SIP Trunks** field to a value that is required for your enterprise.
- Create a node name for Session Manager on the Communication Manager system.

# Add SIP trunk groups

## Adding an SIP trunk group for Communication Manager

### About this task

The trunk group can be either from the Communication Manager Feature Server or from the Communication Manager Evolution Server trunk to Session Manager.

### Procedure

1. At the SAT interface prompt, type **`add trunk-group`** <*nnn*>, where <*nnn*> represents the number of this new trunk group.

    **Note:**

    This number must not be in use. For ease of identification, set this number equal to that of the signaling group that you created. For example, if you created a signaling group as 99, create the corresponding trunk group 99.

    The system displays page 1 of the Trunk Group window.
2. On page 1, set the **Group Type** field to `sip`.
3. On page 1, set the **TAC** field with DAC dialed string that you entered in the dial plan analysis.
4. On page 1, set the **Service Type** field to `tie`.
5. On page 3, set the **Numbering Format** field to `public`.
6. On page 4, set the **Convert 180 to 183 for Early Media?** field to `n`.
7. Save the changes.

# Add SIP signaling groups

## Adding a signaling group for Communication Manager Feature server

### About this task

This task is valid only if you are using Communication Manager as a feature server.

### Procedure

1. At the SAT interface prompt, type `add signaling-group` <*nnn*>, where <*nnn*> represents the number of the new signaling group.

   **Note:**

   The number of this signaling group must not be in use and should also be available for the creation of a trunk group. For example, if you create this signaling group as 99, the corresponding trunk group should be created as 99. For this group, choose a number that is easily differentiated from other signaling and trunk groups.

   The system displays the Signaling Group screen.
2. Set the value of the **Group Type** field to `SIP`.
3. Set the value of the **Transport Method** field to the value you set for the **Protocol** field while administering Session Manager.
4. Set the value of the **IMS Enabled?** field to `y`.
5. Set the value of the **Peer Detection Enabled** field to `y`.
6. Set the value of the **Peer Server** field to `SM`.

   **Note:**

   To edit the **Peer Server** field, first set the **Peer Detection Enabled** field to `n`. After that change the **Peer Detection Enabled** field to `y`.
7. Set the value of the **Near-end Node Name** field to either procr or C-LAN.
8. Set the value of the **Far-end Node Name** field to the node name of Session Manager.
9. Set the value of the **Far-end Domain** field to the domain name specified while administering Session Manager.
10. Set the value of the **DTMF over IP** field to `rtp-payload`.
11. Set the value of the **Enable Layer 3 Test?** field to `yes`.
12. Save the changes.

### Next steps

Update the trunk group page with the signaling group number and the number of members in the signaling group.

## Adding a signaling group for Communication Manager Evolution server

### About this task

This task is valid only if you are using Communication Manager as an evolution server.

### Procedure

1. At the SAT interface prompt, type `add signaling-group` <*nnn*>, where <*nnn*> represents the number of the new signaling group.

   **Note:**

   The number of this signaling group must not be in use and should also be available for the creation of a trunk group. For example, if you create this signaling group as 99, the corresponding trunk group should be created as 99. For this group, choose a number that is easily differentiated from other signaling and trunk groups.

   The system displays the Signaling Group screen.
2. Set the value of the **Group Type** field to `SIP`.
3. Set the value of the **Transport Method** field to the value you set for the **Protocol** field while administering Session Manager.
4. Set the value of the **IMS Enabled** field to `n`.
5. Set the value of the **Peer Server** field to `SM`.

   **Note:**

   To edit the **Peer Server** field, first set the **Peer Detection Enabled** field to `n`. After that change the **Peer Detection Enabled** field to `y`.
6. Set the value of the **Peer Detection Enabled** field to `y`.
7. Set the value of the **Near-end Node Name** field to either procr or C-LAN.
8. Set the value of the **Far-end Node Name** field to the node name of Session Manager.
9. Set the value of the **Far-end Domain** field to the domain name specified while administering Session Manager.
10. Set the value of the **DTMF over IP** field to `rtp-payload`.
11. Set the value of the **Enable Layer 3 Test** field to `yes`.
12. Save the changes.

### Next steps

Update the trunk group page with the signaling group number and the number of members in the signaling group.

## Configuration changes for using Call Admission Control

You can enable Call Admission Control (CAC) between network regions to restrict calls. However, to ensure that CAC works properly, when Communication Manager Messaging is reached over signaling group with a far-end network region different from the network region that Communication Manager Messaging is in, you must make the following changes:

- Duplicate the signaling group used to reach Communication Manager Messaging and change the far-end network region to the appropriate network region in which Communication Manager Messaging is in.
- Duplicate the trunk group used to reach Communication Manager Messaging, and use the new signaling group, and then set the direction to outgoing.
- On the network region administered for Communication Manager Messaging, add an authoritative domain.
- Change the Automatic Alternate Routing (AAR) for the Communication Manager Messaging hunt group so that it uses a new route pattern that routes the call through the new trunk group.

## Changing IP network region

### Procedure

1. At the SAT prompt, type `change ip-network-region n`, where *n* represents the value in the **Far-end Network Region** field.

   The system displays the IP Network Region screen.
2. Set the value of the **Authoritative Domain** field to the SIP domain name.
3. On Page 4, in the **Codec set** column, type `1`.
4. In the **AGL** column, type `ALL`.
5. Save the changes.

## Enable fax

### About this task

It is optional to enable fax.

### Procedure

1. At the SAT interface prompt, type `change ip-codec-set` <*n*>, where <*n*> represents the value you recorded for the Codec Set.
2. On page 2, set the value of the **Fax** field to `t.38-standard`.
3. Save the changes.

## Creating a hunt group for messaging

### Procedure

1. At the SAT interface prompt, type `add hunt-group nnn`, where *nnn* represents the number of a new, unused hunt group.

   This hunt group should be consistent with your country settings, and must be used only for messaging.

   The system displays the Hunt Group screen.

2. Verify that the **Group Name** field is set to `msgserver` for IPv4 IP addresses or `msgserver6` for IPv6 addresses.

3. Verify that the **Group Type** is set to `ucd-mia`.

4. Verify that the **COR** field is set to `1`.

   **Note:**

   The COR for the hunt group must not be outward restricted.

5. Go to page 2.

   **Important:**

   Set the Message Center to the value `sip-adjunct`. This value is required for other fields to display on this page.

6. Verify that the **Message Center** field is set to `sip-adjunct`.

7. Verify that the **Voice Mail Number** field is set to the default voice mail extension.

8. Set the value of the **Voice Mail Handle** field to match the first part of the regular expression you created while administering Session Manager.

   For example, if the regular expression is *cmm@domain.avaya.com*, use *cmm* for the **Voice Mail Handle** field.

9. Verify that the value of the **Routing Digits (e.g. AAR/ARS Access Code)** field matches the FAC that you specified for the **Auto Alternate Routing (AAR) Access Code** field while setting the FACs for messaging.

10. Save the changes.

### Next steps

Change private numbering on page 14.

# Create a route pattern for the new trunk group

## Changing a route pattern

### About this task

**Important:**

For direct SIP switch integration, the route pattern must point to the SIP trunk between Communication Manager and Communication Manager Messaging.

For SIP integration through Session Manager, the route pattern must point to the SIP trunk between Communication Manager and Session Manager.

### Procedure

1. At the SAT interface prompt, type `change route-pattern nnn`, where *nnn* represents the number of the new trunk group that you created while creating a trunk group for messaging. You must enter this number for messaging to function properly.

   The system displays the route-pattern screen.

2. Verify that the fields on this window are appropriate to change the route pattern.

## Route-Pattern field descriptions

| Field | Setting |
|---|---|
| **Pattern Name** | The route pattern name for the messaging trunk group. For example, msgserver. |
| **Grp No.** | The number of the trunk group you created while creating a trunk group between Communication Manager Feature Server/Evolution Server and Session Manager. |
| **FRL** | 0 |
| **DCS/ QSIG Intw** | n |
| **IXC** | user |
| **BCC VALUE**<br>**0 1 2 M 4 W** | y y y y y n |
| **ITC** | rest |
| **Numbering Format** | The numbering format of the trunk group. |
| **LAR** | rehu |

## Changing AAR analysis

### Procedure

1. Enter `change aar analysis n`, where *n* represents the first digit of the messaging extension.

The system displays the AAR DIGIT ANALYSIS TABLE screen.

2. Verify that appropriate values are set on Page 1.

   **Important:**

   You must use values that are appropriate for your configuration. A system may use *n*–digit extensions. For example, the default messaging voice mail extension number is 30000. This number varies for every site. The columns for **Total Min** and **Total Max** refer to the number of digits in the voice mail extension. If you are using a dial plan with more than five digits, you must adjust this number accordingly.

3. Save the changes.

### Next steps

Save translations on page 16.

# Communication Manager Messaging administration

## Administering switch link for SIP integration through Session Manager

### About this task

Perform the following steps on the Communication Manager Messaging System Management Interface.

### Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the left navigation pane, click **Switch Link Admin**.
4. In the **Extension Length** field, select the appropriate length or select **Variable** for variable extensions.

   **Note:**

   The extension length must match the length assigned to the station on Communication Manager.

5. In the **SIP Domain** field, type the domain used for Communication Manager and Communication Manager Messaging while administering Session Manager.
6. In the **Far-end Connections** field, type the number of Session Manager virtual machines you want to use for the SIP integration of Communication Manager Messaging. You can

have more than one Session Manager. Depending on the value you select the page displays those many fields to type the IP addresses of Session Manager.

7. In the **Connection_n** field, type the Asset IP address of Session Manager, the port number that was administered on Session Manager for the entity link, transport type, and monitor interval for each connection.
8. The **Messaging Address** field, displays the IP address of Communication Manager Messaging. You also need to type the **TCP port** number that was administered on Session Manager for the entity link.
9. In the **Messaging Ports** field, type the number of call answer ports to configure.
10. In the **Switch Trunks** field, type the total number of trunks for Communication Manager.
11. Click **Show Advanced Options**.

    The system displays advanced options that you might need to administer.
12. In the **Quality of Service** field, type a value for Call Control Per Hop Behavior (PHB) and Audio PHB or accept the default values.

    The value you enter for both the fields sets the quality of service level for call control messages and audio streams respectively on networks that support this feature. The value for both the fields must be in the range 0 to 63. The value must match the corresponding number configured for the network region used by the messaging signaling group on the switch.
13. In the **UDP Port Range** field, enter a starting UDP port number for RTP.

    The end port number is calculated automatically.
14. If you have configured SRTP for messaging, in the **Media Encryption** field, select the type of Secure Real-time Transport Protocol (SRTP) encryption for messaging. To select a **Media Encryption**:

    a. In the **Media Encryption** row, click **Clear** to remove the default value **1 : None**.

    b. Select the SRTP, you have configured for messaging, from the list and click **Add**.

    **Important:**

    You must enable the SRTP feature in the change customer-options form and set the media encryption type in the change ip-codec-set form on Communication Manager.
15. To enable DTMF transport via SIP INFO method, in the **SIP INFO FOR DTMF** field, select `Accept`.

    **Important:**

    You must set the **DTMF over IP** field to `out-of-band` on the Communication Manager **SIGNALING GROUP** screen.

    **Note:**

    This field is set to Ignore. If you change it to Accept, then any digits received from rtp-payload will be ignored.

16. Click **Save**.

## Restarting the Communication Manager Messaging application

### Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the left navigation pane, under **Utilities**, click **Stop Messaging**.

   The system displays the Stop Messaging Software page.

   The shutdown is delayed until all calls are completed. The system will end all calls that remain three minutes after beginning shutdown.
4. Click **Stop**.

   The system displays a message to indicate that Messaging is stopped.
5. After the application stops, click **Start Messaging**.

### Next steps

Complete the steps in the *Testing Communication Manager Messaging* section.

# Chapter 5: Administering CMM System Parameters

## Setting Communication Manager Messaging server parameters

### Procedure

1. Log in to Communication Manager Messaging System Management Interface.
2. Select **Administration** > **Messaging**.
3. In the navigation pane, under the **Server Administration** group, click **Messaging Server Admin**.

   The system displays the Edit Messaging Server screen.
4. In the **Server Name** field, verify that the server name matches the Host name you have specified while deploying Communication Manager Messaging OVA.
5. In the **Password** and **Confirm Password** fields, type a password for other messaging servers to use to access the messaging server that you selected.
6. **(Optional)** If servers have overlapping mailbox numbers, enter prefix digits in the **Prefix** field to distinguish between the servers.

   The prefix can be 0 to 21 alphanumeric characters in length.
7. In the **Starting Mailbox Number** and the **Ending Mailbox Number** fields of the MAILBOX NUMBER RANGES table, enter the starting and ending extensions that are assigned to this call center.

   ✱ **Note:**

   You can setup variable extensions in 7.0. **Starting Mailbox Number** and **Ending Mailbox Number** lengths must be same while administering variable length extensions.

   The range for the **Starting Mailbox Number** and **Ending Mailbox Number** must be between 0 to 9.
8. Verify that the **IP address** field contains the IP address of the Communication Manager Messaging virtual machine.
9. Verify that the **Server Type** field is set to `tcpip`.
10. Verify that the **Voiced Name** field is set to `NO`.

11. Verify that the **Extension Length** field is set to the value used in the dial plan for this site.
12. Verify that the **Voice ID** field is set to `0`.
13. Verify that the **Default Community** is set to `1`.
14. Click **Save**.

    The system displays the message `Server information modified successfully`.

## Setting system-wide Messaging parameters

### Procedure

1. Log in to Communication Manager Messaging System Management Interface.
2. Select **Administration** > **Messaging**.
3. Click **Server Administration** > **System Administration**.

   The system displays the Administer System Attributes and Features screen.
4. In the **Lock Duration** field, type the length of time a mailbox remains locked after the administered number of failed login attempts.
5. In the **Consecutive Invalid Attempts** field, type the number of login attempts allowed before a mailbox is locked.
6. In the **Minimum Password length** field, type the minimum number of digits that subscriber passwords must contain.
7. In the **Passwords History** field, type the number of old passwords that the system saves to check against old password reuse by a subscriber.
8. In the **Passwords Expiration Interval** field, type the number of days a subscriber password is valid, after which the system requires the subscriber to change the password.
9. Click **Save**.

# Chapter 6: Testing Communication Manager Messaging

## Adding test subscribers for messaging

### About this task

For each test subscriber, you must administer the telephones on the Communication Manager server. The following procedure creates a mailbox associated with each subscriber's telephone.

Create two subscribers to perform the initial testing of your messaging software.

### Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the left navigation pane, under the select **Messaging Administration** group, click **Subscriber Management**.

   The system displays the Manage Subscribers screen.
4. In the **Local Subscriber Mailbox Number** field, type the extension number of the first test subscriber.
5. Click **Add** or **Edit**.

   The system displays the Add Local Subscriber screen.
6. In the **First Name** field, type the first name of the first test subscriber.
7. In the **Last Name** field, type the last name of the first test subscriber.
8. In the **Password** field, type the password for the subscriber's mailbox.
9. Ensure that the **Mailbox Number** field displays the number you administered in the **Extension Length** field on the Switch Link Administration screen.
10. In the **Class Of Service** field, select the appropriate **Class Of Service**.
11. Click **Save**.
12. Repeat the steps for the second test subscriber mailbox.

# Verify the messaging application

You must verify that the Messaging application is functioning properly after you configure the Messaging virtual system.

# Calling the hunt group to setup test mailbox

### Procedure

Place a call from one of the stations to the messaging hunt group number.

You should hear the greeting `Welcome to Audix`. If you do not hear this greeting, ensure that the settings for the hunt group, coverage path, station, and subscriber are set properly.

# Calling an extension to leave a test message

### Procedure

1. Make a call from the first station to the second station.
2. Do not answer the call.

   Your call will route to the messaging system and you should be able to leave a voice message to the second station. If you do not hear the system prompt asking you to leave a message, ensure that the settings for the hunt group, coverage path, station, and subscriber are set properly.

   **Note:**

   Ensure that the **Message Waiting Indicator** on the second station turns on and the user can review the new message.

# Chapter 7: Related resources

## Documentation

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

| Document number | Title | Description | Audience |
|---|---|---|---|
| Deployment | | | |
| | *Deploying Avaya Aura® Communication Manager Messaging* | Describes the deployment instructions for Communication Manager Messaging. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| | *Deploying Avaya Aura® applications from Avaya Aura® System Manager* | Describes the deployment instructions for Avaya Aura® using Solution Deployment Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| Implementation | | | |
| | *Implementing Avaya Aura® Communication Manager Messaging* | This document describes the implementation process of Communication Manager Messaging. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| Upgrade | | | |
| | *Upgrading and Migrating Avaya Aura® applications to Release 7.0* | Describes the upgrade for Avaya Aura® using Solution Deployment Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |
| Administration | | | |
| | *Avaya Aura® Communication Manager Screen Reference*, 03-602878 | Describes the screens and fields of Communication Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel |

*Table continues…*

| Document number | Title | Description | Audience |
|---|---|---|---|
| | *Administering Avaya Aura® Session Manager* | Describes the administration instructions for Session Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel, Administrators |
| | *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504 | Describes the network connectivity for Communication Manager. | Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel, Administrators |

# Finding documents on the Avaya Support website

## About this task

Use this procedure to find product documentation on the Avaya Support website.

## Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

# Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

| Course code | Course title |
|---|---|
| **Understanding** | |
| 1A00234E | Avaya Aura® Fundamental Technology |
| AVA00383WEN | Avaya Aura® Communication Manager Overview |
| ATI01672VEN, AVA00832WEN, AVA00832VEN | Avaya Aura® Communication Manager Fundamentals |
| 2007V | What is New in Avaya Aura® 7.0 |
| 2009V | What is New in Avaya Aura® Communication Manager 7.0 |
| 2011V | What is New in Avaya Aura® System Manager & Avaya Aura® Session Manager 7.0 |
| 2009T | What is New in Avaya Aura® Communication Manager 7.0 Online Test |
| 2013V | Avaya Aura® 7.0 Solution Management |
| 5U00060E | Knowledge Access: ACSS - Avaya Aura® Communication Manager and CM Messaging Embedded Support (6 months) |
| **Implementation and Upgrading** | |
| 4U00030E | Avaya Aura® Communication Manager and CM Messaging Implementation |
| ATC00838VEN | Avaya Media Servers and Implementation Workshop Labs |
| AVA00838H00 | Avaya Media Servers and Media Gateways Implementation Workshop |
| ATC00838VEN | Avaya Media Servers and Gateways Implementation Workshop Labs |
| 2012V | Migrating and Upgrading to Avaya Aura® 7.0 |
| **Administration** | |
| AVA00279WEN | Communication Manager - Configuring Basic Features |
| AVA00836H00 | Communication Manager Basic Administration |
| AVA00835WEN | Avaya Communication Manager Trunk and Routing Administration |
| 5U00041I | Avaya Aura® Communication Manager Administration |
| AVA00833WEN | Avaya Communication Manager - Call Permissions |
| AVA00834WEN | Avaya Communication Manager - System Features and Administration |
| 5U00051E | Knowledge Access: Avaya Aura® Communication Manager Administration |

# 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.

### Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  ✱ **Note:**

  Videos are not available for all products.

# Support

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

# Index