Implementing Avaya Aura®
Communication Manager Messaging

Release 6.3
18-603644
May 2013

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software ("Product(s)"). 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: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; 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. "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.

License types

- Designated System(s) License (DS). End User may install and use each copy 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, 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.
- Database License (DL). End User may install and use each copy 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 a single instance of the same database.
- CPU License (CP). End User may install and use each copy 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 the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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.

Virtualization

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that 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"). 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 Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

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

Trademarks

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

Avaya and Avaya Aura® are trademarks of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document describes the implementation process for Communication Manager Messaging 6.3.

Intended audience

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

Document changes since last issue

The following changes have been made to this document since the last issue:

- Avaya recommends direct SIP integration between Communication Manager Messaging and Communication Manager as from Release 6.3, H.323 integration is deprecated.

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
Implementation			
18-603644	Implementing Avaya Aura® Communication Manager Messaging	Describes the implementation instructions for Communication Manager Messaging.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Migration			
18-603649	Migrating from Intuity™ Audix® LX R1.1 to Avaya Aura® Communication Manager Messaging R6.3	Describes the migration scenario for Communication Manager Messaging.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
18-603650	Migrating from Intuity™ Audix® LX R2.0 to Avaya Aura® Communication Manager Messaging R6.3	Describes the migration scenario forCommunication Manager Messaging.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Training

The following courses are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go** .

Course code	Course title
ATI01731VEN	Avaya Aura® Communication Manager Messaging Embedded Implementation
5M00050V	Avaya Aura® Communication Manager Messaging Embedded Administration, Maintenance and Troubleshooting

Avaya Mentor videos

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

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

- Enter a key word 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 site.

Support

Visit 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.

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: Communication Manager Messaging

Overview

The Communication Manager Messaging embedded application comes packaged as part of the solution templates that are used to install Communication Manager. There is no hardware requirement for the Communication Manager Messaging embedded application since it is installed as part of the solution template for Communication Manager.

The Communication Manager solution template is installed after installing Avaya Aura®System Platform software on an S8800 Server, S8300D Server, S8510 Server, Dell™ PowerEdge™ R610, or an HP ProLiant DL360 G7 1U. The System Platform can host one or more virtual machines.

Integration of the Communication Manager Messaging application with Communication Manager happens through the H.323/Q.Sig protocol or through the SIP protocol.Communication Manager supports Session Initiation Protocol (SIP) endpoints if you choose the integration protocol as SIP.

Supported solution templates and servers

- Simplex Survivable Core on an S8800 Server, S8510 Server, Dell R610, or an HP DL360 G7
- Embedded Survivable Core on an S8300D Server

Important:

Avaya recommends direct SIP integration between Communication Manager Messaging and Communication Manager as from Release 6.3, H.323 integration is deprecated.

IPv6

Internet Protocol version 6 (IPv6) is the successor to IPv4. IPv6 supports 128–bit addresses and satisfies the rapidly growing demand for IP addresses. In contrast, IPv4 supported 32–bit. IPv6 also improves security, ease of configuration, and routing performance. IPv6 can coexist with IPv4 networks, easing the transition process.

The IETF (Internet Engineering Task Force) published RFC 2460, the internet standard specification that defines IPv6, in December 1998.

Addressing

By using 128-bit addresses, IPv6 has about 3.4×10^{38} unique IP addresses, more than enough for every network device. This eliminates the IPv4 mechanisms, such as NAT (network address transitions), that are used to relieve IP address exhaustion. IPv6 addresses are normally written as hexadecimal digits with colon separators, for example: 2005:af0c:168d::752e:375:4020. The double colon "::" represents a string of zeroes, according to RFC4291.

Simplicity

IPv6 simplifies the routing process by changing the packet header and packet forwarding:

- Simplified packet header, despite enhanced functionality.
- IPv6 routers do not perform fragmentation. This is carried out by IPv6 hosts.
- IPv6 routers do not need to recompute a checksum when header fields change.
- Routers no longer need to calculate the time a packet spent in a queue.
- IPv6 supports stateless address configuration, so IPv6 hosts can be configured automatically when connected to a routed IPv6 network through ICMPv6. Stateful configuration using DHCPv6 and static configuration are also available.

Deployment and transition

There are several mechanisms that ease the deployment of IPv6 running alongside IPv4. The key to the transition is dual-stack hosts. Dual-stack hosts refers to the presence of two IP software implementations in one operating system, one for IPv4 and one for IPv6. These dual-stack hosts can run the protocols independently or as a Hybrid. The Hybrid is the common form on recent server operating systems and computers.

When an IPv6 host or network must use the existing IPv4 infrastructure to carry IPv6 packets, *Tunneling* provides the solution. Tunneling encapsulates IPv6 packets within IPv4. Tunneling can be either *automatic* or *configured*, the latter being more suitable for large, well-administered networks.

Key differences between IPv4 and IPv6

	IPv4	IPv6
Address space	32-bit, about 4.3×10^{9}	128-bit, about 3.4×10^{38}
Security	IPSec support is optional.	IPSec support is required.
Configuration	Requires DHCP or manual configuration.	Stateless auto-configuration. Does not require DHCP or manual configuration.
Address format	Decimal digits with colon separators, for example: 192.168.1.1	Hexadecimal digits with colon separators. For example: 2005:af0c:168d::752e:375:4020. The double

		colon “::” represents four zeros “0000”
Broadcast and Multicast support	Yes	No Broadcast. Various forms of Multicast — better network bandwidth efficiency
QoS support	ToS using DIFFServ	Flow labels and flow classes, more granular approach.

Feature Support in Avaya Branch Gateways

Certain Branch Gateway features are not supported in IPv6.

Enabling IPv6 format on the gateway

Procedure

1. Using PuTTY, log in to the gateway using `root` credentials.
2. At the prompt, type **`interface VLAN 1`**.
3. Press `Enter`.
4. Type **`icc-vlan`**.
5. Press `Enter`.
6. Type **`ipv6 admin-state up`**.
7. Press `Enter`.
8. Type **`PMI6`**.
9. Press `Enter`.
10. Type `exit`.

Adding IP address in IPv6 format of Communication Manager

Procedure

1. At the prompt, type **`clear mgc list`**.
2. Press `Enter`.
3. Type **`show mgc list`**.
4. Press `Enter`.

5. Type **set mgc list** *IPv4 address* + *IPv6 Address* of Communication Manager.
6. Press `Enter`.
7. Type **copy run start**. This command copies the configuration to the gateway.
8. Type **reset**.
   The gateway is registered to Communication Manager with IPv6 capability.

Prerequisite

Installing the license file

To implement the features of Communication Manager Messaging, you need to install the license file before installing the Communication Manager template. Starting R6.0, Product Licensing and Delivery System (PLDS), a common license generation and management platform shared by other Avaya Aura® products, generates and manages licenses. You must raise a request in SAP for a specific license. PLDS then maps your request to entitlements. You will receive an email notification with a license activation code (LAC) once your request has been processed.

Procedure

1. Log in to WebLM through System Platform Console Domain using `craft` login.

   Important:
   You must change the password on first login.
2. In the left navigation pane, click **Server Properties**.
3. Click **Install License**.
4. Click **Browse** to locate the license file.
5. Click **Install**.

Verifying license installation

Procedure

1. Log in to Communication Manager Web interface (SMI).

2. Click **Administration** > **Licensing**.
3. In the left hand pane, click **License Status**.
4. Verify that **Messaging License Mode** is Normal

Support

Visit 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.

Chapter 3: Administering Communication Manager for Communication Manager Messaging

Communication Manager installation

For information on installing and configuring Communication Manager.

See*Installing and Configuring Avaya Aura® Communication Manager*, Release 6.2.

Accessing the Messaging virtual machine

Using the SSH connection type

Before you begin

Install PuTTy to gain access to the virtual system.

Procedure

1. Open the PuTTY application.
2. Select SSH as the connection type.
3. Enter the IP address of the virtual system.
4. Click **Open**.

Next steps

Log in to the virtual machine.

Logging in to the virtual system

Procedure

1. Log in as **`craft`**.
2. At the craft *servername*> prompt, enter `su - root`.
3. Enter the password.
4. At the root@*servername*] # prompt, enter `cmm`.
   The system logs you into the virtual system.

Accessing the System Management Interface

About this task

You can gain access to SMI remotely through the corporate LAN connection, or directly from a portable computer connected to the server through the services port.

If the server is not connected to the network, you must access the SMI directly from a portable computer connected to the server through the services port.

Procedure

1. Open a compatible Web browser.

   Currently, SMI supports Internet Explorer 7.0, and Mozilla Firefox 3.6 and later.
2. In your browser, choose one of the following options depending on server configuration:
   - LAN access by IP address

     To log on to the corporate LAN, type the unique IP address of the S8xxx Server in the standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a domain name service (DNS) server that is administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     To log on to the services port from a directly connected portable computer, the IP address must be that of the IP address of the Communication Manager server.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you see a warning with instructions to load the security certificate. If you are certain your connection is secure, accept the server security certificate to access the Logon screen. If you plan to use this computer and browser to access this or other S8xxx Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type your user name.

   Note:

   If you use an Avaya services login that is protected by the Access Security Gateway (ASG), you must have an ASG tool to generate a response for the challenge that the Logon page generates. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

5. Click **Continue**.
6. Type your password, and click **Logon**.

   After successful authentication, the system displays the home page of the Communication Manager SMI.

Enabling messaging

Procedure

1. Open a compatible Web browser.
2. In the **Address (or Location)** field, type the IP address or name of the virtual system and press **Enter**. For example, http://serverIPaddress.com.
3. Log in as craft.
   The system displays the System Management Interface Web page
4. Click **Administration** > **Server (Maintenance)**.
5. Click **Miscellaneous** > **Messaging Software**.

6. Click **Enable**.

Patch management

Patch installation overview

A Service Pack provides product updates and bug fixes. When a Service Pack is available on the Avaya Support website, the supporting information clearly states the issues addressed in the Service Pack. Even if you do not have problems, implement the Service Packs to keep the systems up-to-date and minimize the likelihood of future issues.

A patch provides critical security, performance, and stability fixes or updates. A Service Pack is a bundle of updates, fixes, enhancements, and previously released patches. In this document, the word *patches* refers to both patches and Service Packs.

You can install, download, and manage the patches from the System Platform Web Console.

You must install the following patches in addition to the currently installed software:

- Communication Manager: You must install Communication Manager patches because Communication Manager Messaging uses the Communication Manager platform that requires software updates.
- Communication Manager Messaging

You must install the following patches when available:

- Security
- Kernel

Important:

Install kernel updates only during a planned downtime for system maintenance.

To download the latest patches and to obtain the necessary information, see *Avaya Aura® Messaging Release Notes* on the Avaya Support website at https://support.avaya.com/Products/P0792.

Important:

Before you apply a patch, back up the system. When you install the latest patch, the installation program automatically uninstalls the previous patch. So if you remove a patch, the removal does not reinstall the previous patch or revert the system to the previous state, that is, the state before the patch was installed. To revert the system to the previous state, you must reinstall the previous patch.

For more information, see the “Backup and restore” section of *Administering Avaya Aura® Messaging*.

Caution:

Patch installation process affects the availability of the Messaging service.

Installing patches

Before you begin

Ensure that the Messaging system is running.

Procedure

1. Log on to the System Platform Web Console.
2. Click **Server Management** > **Patch Management** > **Download/Upload**.
   The system displays the Search Local and Remote Patch page.
3. From the **Choose Media** drop-down list, select the medium to search for a patch.
   The following table lists the available options.

Option	Action
Avaya Downloads (PLDS)	Provide **SSO Login** and **SSO Password** and then click **Search**. **Note:** This option is not available for Avaya Services.
HTTP	Specify the **Patch URL** and click **Search**. If the patches are located on a different server, you might have to configure a proxy depending on your network. Click **Configure Proxy** to specify a proxy server if required.
SP Server	Specify the **Patch URL** and click **Search**. **Note:** This option is not available for Avaya Services.
SP CD/DVD	Click **Search**.
SP USB Disk	Click **Search**.
Local File System	Click **Add** to locate the patch file on your computer and then click **Upload**.

   For more information, see Search Local and Remote Patch field descriptions on page 24.

   The system displays the Select Patches page.

4. From the **Select Patches** list, select the patch that you want to download.
5. Click **Select**.
   The system displays the Patch Detail page.
6. On the Patch Detail page, click **Install**.
   For more information, see Patch Detail field descriptions on page 26.
   The Patch Detail page displays the progress of the patch installation process.

Next steps

Verify the patch installation.

Search Local and Remote Patch field descriptions

Name	Description
Supported Patch File Extensions	The patch that you select for installing. Ensure that the patch matches the extensions in this list. For example, *.tar.gz,*.tar.bz,*.gz,*.bz,*.zip,*.tar,*.jar,*.rpm,*.patch.
Choose Media	The media options from where you can search for a patch The available options are: • **Avaya Downloads (PLDS)** Download the patch files located on the Avaya Product Licensing and Delivery System (PLDS) website, you must enter an Avaya SSO login and password to access this site. The list on this site contains all the templates that your company is entitled to. Each line in the list begins with the sold-to number. Use the sold-to number to select the appropriate template for your site. For more information about a sold-to number, hold the mouse pointer over the number. • **HTTP** Download the patch files located on an HTTP server, you must enter the patch location information. • **SP Server**: Download the patch files located in the `/vsp-template` directory in the Console Domain of the System Platform server, you must specify the patch location for the server.

Name	Description
	Tip: When you move files from a laptop to the System Platform Server, you may encounter some errors, as System Domain (Dom–0) and Console Domain support only SCP. Most laptops do not support SCP. To enable SCP, download the following two programs: - Pscp.exe - WinSCP For detailed procedures on how to download the programs, search the Internet. • **SP CD/DVD** Download the patch files located on a CD-ROM or DVD in the CD/DVD drive on the System Platform server. • **SP USB Disk** Download the patch files located on a USB flash drive connected to the server. • **Local File System** Download the patch files located in a local file system.
SSO Login	The log-in ID to log on to Single Sign On. The system activates this field only when you select the **Avaya Downloads (PLDS)** option to search for a patch.
SSO Password	The password for Single Sign On. The system activates this field only when you select the **Avaya Downloads (PLDS)** option to search for a patch.
Patch URL	The URL of the server where the template files are located. The system activates this field only when you select the **HTTP** or **SP Server** option to search for a patch.

Patch Detail field descriptions

Name	Description
ID	The file name of the patch file.
Version	The version of the patch file.
Product ID	The name of the virtual machine.
Description	The short description of the patch file.
Detail	The virtual machine name for which the patch is applicable. This field is not applicable for Communication Manager Messaging patches.
Dependency	The dependency that the patch file might have on any other file, if any. This field is not applicable for Communication Manager Messaging patches.
Applicable for	The software load for which the patch is applicable. This field is not applicable for Communication Manager Messaging patches.
Service effecting when	The action (if any) that causes the selected patch to restart the Communication Manager Messaging services.
Restart this console when	The conditions or circumstances when the System Platform Web Console must be restarted. This field is not applicable for Communication Manager Messaging patches.
Disable sanity when	The stage at which the condition is set to disable. This field is not applicable for Communication Manager Messaging patches.
Status	The status to show whether the patch is available for installation or already installed.
Patch File	The path where the patch is cached on the Console Domain.

Verifying the patch installation

Procedure

1. Click **Server Management** > **Patch Management** > **Manage**.
   The system displays the Patch List page.
2. Verify that the patches you installed (Communication Manager Messaging and Communication Manager) are displayed under the *cmm* heading and the status of the patch is **Active**.
   For more information, see Patch List field descriptions on page 27.

Patch List field descriptions

The Patch List page displays the patches on the System Platform server for installation or removal. To view the details of the patch file, click the file name.

Name	Description
System Platform	Lists the patches available for System Platform.
Solution Template	Lists the patches available for the respective solution templates.
cmm	Lists the patches available for Communication Manager Messaging.
Patch ID	Lists the file name of a patch.
Description	Provides information on a patch. For example, describes a patch available for System Platform as: SP patch.
Status	Shows the status of a patch. The possible values of **Status** are **Active** and **Not Installed**.
Service Effecting	Shows if installing the patch causes the Communication Manager Messaging virtual machine to reboot.

Removing patches

Procedure

1. Click **Server Management** > **Patch Management** > **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

2. On the Patch List page, click a patch that you want to remove.
3. On the Patch Detail page, you can:
   - Click **Remove** to uninstall the patch.
   - Click **Remove Patch File** to clean up the hard disk drive by deleting the installation file for an uninstalled patch.

Administering Communication Manager for Communication Manager Messaging

Connecting to the Communication Manager server SAT interface

About this task

Use this procedure to connect your configured laptop computer to the Communication Manager virtual machine and to start the System Administration Terminal (SAT) interface.

Procedure

1. Connect your laptop computer to the services port of the server using a CAT5 ethernet cable.
2. Use a SSH session to access `192.11.13.6`.
3. Log in as **`craft`**.
   The system displays the SAT interface.

Checking customer options for the Communication Manager server

About this task

Use these forms to ensure that the features are appropriately set or and the necessary H.323 and messaging options are 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.

Note:

On the SAT interface, press`Control (+) N` to navigate to the next screen and the `Control (+) P` to go to a previous screen.

Procedure

1. At the SAT interface prompt, enter **`display system-parameters customer-options`**.
   The system displays page 1 of the OPTIONAL FEATURES window.
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 locate the **Maximum Administered H.323 Trunks** field.
4. Check that the quantity in the first column of the Maximum Administered H.323 Trunks field is set to a number that can accommodate the sum of the following:
   - The busy hour number of H.323 connections required by the Communication Manager port networks, including port network-to-port network voice connections, port network– to– media gateway voice connections, and Communication Manager Server-to-Communication Manager Server voice connections.
   - The number of voice ports and transfer ports (normally 50% of voice ports) for CM Messaging.
5. Verify that the **Maximum Administered SIP Trunks** field is set to the appropriate value.
6. Go to page 3.
7. Verify that the **ARS?** and **ARS/AAR Partitioning?** fields are set to `y`.
8. Go to page 4.
9. Verify that the **IP Trunks?** and **ISDN-PRI?** fields are set to `y`.
10. Go to page 5.
11. Verify that the **Private Networking?**, **Processor Ethernet?**, and **Uniform Dialing Plan?** fields are set to `y`.
12. Go to page 8.
13. 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`.

14. Press the key combination `Control E` to save the values in the window.

Setting feature access codes for messaging

About this task

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

Procedure

1. Go to the SAT interface prompt and enter **`change dialplan analysis`**.
   The system displays the DIAL PLAN ANALYSIS TABLE window.
2. Create two FACs. The FACs that you use for messaging can be one or more digits.

   For example, in the following screen, Dialed Strings 8 and 9 are specified as FACs, and Dialed String 1 is specified 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. Press the key combination `Control E` to save the changes and exit the window.
4. Go to the SAT interface prompt and enter **`change feature-access-codes`**.
   The system displays the FEATURE ACCESS CODE (FAC) window.
5. Verify that the **Auto Alternate Routing (AAR) Access Code** field is set to the first FAC Dialed String value you entered for 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 3.
6. Verify that the **Auto Route Selection (ARS) - Access Code 1** field is set to the second FAC Dialed String value you entered for 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. Press the key combination `Control E` to save the changes and exit the window.

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 enter **`change system-parameters features`**.
   The system displays the FEATURE-RELATED SYSTEM PARAMETERS window.
2. Verify that the **Trunk-to-Trunk Transfer** field is set to `all`.
3. Go to page 8.
4. 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 messaging?**
   - **Maximum Length**
   - **QSIG Path Replacement Extension**
   - **Path Replace While in Queue/ Vectoring?**
5. Click **Submit** to save the values set in this window.
6. Go to the SAT interface prompt and enter **`change dialplan parameters`**.
   The system displays the Dialplan Parameters window.
7. Verify that the **Local Node Number** is set to the proper values for the installation site.

   Local Node Number is the number for this communication server. Usually this number is 1, but it can be a number from 1 to 99, depending on your contact center configuration.
8. Press the key combination `Control E` to save the values set on this window.
9. Go to the SAT interface prompt and enter **`change node-names ip`**.
   The system displays the IP NODE NAMES window.
10. Enter the name of the Communication Manager Messaging server in the next available **Name** field. You can enter the name as required for the IP address version, IPv4 or IPv6.
11. The **Messaging** field displays the IP address of Communication Manager.

    Important:

    The Communication Manager Messaging name must be consistent between the IP node names and the signaling group assigned for messaging.

12. Check the list of interfaces for existing Processor Ethernet (PROCR) or CLAN interfaces.

    Note:

    CLAN functionality is deprecated.

    If a PROCR or a CLAN interface does not exist, you need to create the required interface on this window and assign it an IP address.

    When both the Processor Ethernet and CLAN interfaces are available on a system, you may base the decision on which interface to use for messaging communications on factors such as:

    - Whether or not a survivable core server is being used for reliability. A survivable core server can support messaging in the event of a Communication Manager server failure only if messaging uses the CLAN interface.
    - Load balancing. If media gateways, IP telephones, or other devices have the CLAN as the primary interface to Communication Manager, then the Processor Ethernet interface may be preferable to the CLAN interface.

13. Press the key combination `Control E` to save the values set on this window.

Feature-Related System Parameters window field descriptions

Parameter name	Description
IQSIG/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 messaging?	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.

Parameter name	Description
Maximum Length	When the Unknown Numbers Considered Internal for messaging? field is set to `y`, the Maximum Length field is displayed to the right. 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. 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`. 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 server communicates with the Communication Manager server through the Processor Ethernet (PROCR) port of the server itself.

Note:

The functionality to administer Control LAN (CLAN) circuit pack installed on a port network as an IP interface is deprecated.

Defining IP interfaces for Processor Ethernet

Procedure

1. Enter **`change ip-interfaces procr`**.
   The system displays the IP Interfaces window.

2. Enter values for the fields in the window.

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 *Administration for Network Connectivity for Avaya 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 its 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.
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 a yes on this form.

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 *Administration for Network Connectivity for Avaya 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 enter **`change system-parameters coverage`**.
   The system displays the SYSTEM PARAMETERS CALL COVERAGE / CALL FORWARDING window.
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 Incomming 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. Press the key combination `Control E` to save changes made to the window.

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 enter `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

3. Press Control E to save changes.

AAR and ARS digit conversion

Depending on the **Format** field setting on Page 3 of the Trunk Group window, 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, enter `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. Press the key combination `Control E` to save the values set in the window.
4. At the SAT interface prompt, enter `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, enter **`save translation`**.
The system saves the translations.

Chapter 4: Administer SIP or H.323 switch integration

Administer SIP or H.323 integration type for Communication Manager Messaging

You can administer Communication Manager Messaging for either SIP protocol or H.323 protocol integration. You can administer SIP integration either via Session Manager or a direct SIP integration with Communication Manager.

Important:

Communication Manager Messaging only support the following DTMF sets while creating signaling groups for the following integrations:

- H.323 integration only supports **out-of-band** as the DTMF set.
- SIP integration supports **out-of-band** as the DTMF set if **SIP INFO for DTMF** is set to **Accept**. It supports **rtp-payload** as the DTMF set if **SIP INFO for DTMF** is set to **Ignore**.

Direct SIP integration between Communication Manager Messaging and Communication Manager

Overview

Communication Manager Messaging allows direct SIP integration with Communication Manager. You need to administer Communication Manager screens and Communication Manager Messaging Web pages to implement direct SIP integration between Communication Manager and Communication Manager Messaging.

Adding node names for SIP integration

Procedure

1. Using PuTTY, log in to the SAT screen.
2. Type **`change node-names ip`**.
3. In the **Names** column, add an entry for SIP.
4. Type `procr`.
5. In the **IP Address** column, enter the IP address of the processor Ethernet.
6. Type `msgserver` for IPv4 IP addresses or `msgserver6` for IPv6 addresses.
7. In the **IP Address** column, enter the same IP address that you entered for the processor Ethernet.
8. Submit the changes.

Adding a signaling group for direct SIP integration

Procedure

1. On the SAT command prompt, type **`add signaling-group`** *n*, where *n* is the signaling group used for SIP.
2. On Page 1 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 **Far-end Node Name** field, type `msgserver`.
6. In the **Far-end Listen Port** field, type a value that is different from the value entered in the **Near-end Listen Port** field. You can use 5060/6060 (near-end listen port/far-end listen port) as the port numbers for TCP transport type and 5061/6061 (near-end listen port/far-end listen port) as the port numbers for TLS transport type.
7. In the **Far-end Network Region** field, type `1`.
8. In the **Far-end Domain** field, type the SIP domain name.

   Note:

   Ensure that you enter the same values on the Adding signaling group form and the Switch Link Admin Web page of the Communication Manager Messaging Web interface.

9. Submit 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) or name of the `CLAN`, 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	6060 (TCP) / 6061(TLS)
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. • `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
Interworking Message	PROGress

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.

The field, Far-end Network Region, defaults to 1 if a value is not specified.

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 value 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. Submit the changes.

Creating a hunt group for messaging

Procedure

1. At the SAT interface prompt, enter **`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. It is only used for messaging.

   The system displays the Hunt Group window.
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. Press the key combination `Control E` to save the values in the window.

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 enter `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

3. Press Control E to save changes.

Changing a route pattern

About this task

Important:
The route pattern must point to the SIP trunk between Communication Manager and Communication Manager Messaging.

Procedure

1. Go to the SAT interface prompt, enter **`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 window.
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 **0 1 2 3 4 W**	y y y y y n
TSC	y
CA-TSC Request	none

Field	Setting
ITC	rest
LAR	rehu

Note:

The **CA-TSC Request** field cannot contain a value until the **TSC** field is set to `y`.

Changing IP network region

Procedure

1. At the SAT interface prompt, enter `change ip-network-region` <*n*>, where <*n*> represents the value in the **Far-end Network Region** field.
2. Press `Enter`.
   The system displays the IP Network Region page.
3. Set the value of the **Authoritative Domain** field to the SIP domain name.
4. On Page 4, in the **Codec set** column, type `1`.
5. In the **AGL** column, type `ALL`.
6. Save the changes.

Changing the IP Codec Set

Procedure

1. At the SAT interface prompt, enter **change ip-codec-set** <*n*>, where <*n*> represents the value you recorded for the Codec Set.
   The system displays the IP Codec Set window.
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.
5. 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`.

6. Press the key combination `Control E` to save the values on the window.

Adding a coverage path for messaging

Procedure

1. At the SAT interface prompt, enter **`add coverage path`** <*nnn*>, where <*nnn*> represents the number of a new, unused coverage path. You can substitute <*nnn*> with 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 window.
2. In the Point1 field, enter **`h`***xx*, where *xx* is the hunt group you created for messaging.

   For example, h3 represents hunt group 3.
3. Press the key combination `Control E` to save the values in the window.

Changing AAR analysis

Procedure

1. Enter **`change aar analysis`** <*n*>, where *n* represents the first digit of the welcome to messaging extension.
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 per 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. Submit the changes.

Adding a station

Procedure

1. On the SAT form, type **`add station`** <*n*>, where <*n*> is the a number from the range of extension for your enterprise.
2. In the **Type** field, type the station type.
3. In the **Coverage Path 1** field, type the coverage path number that was set while adding the coverage path.
4. In the **Security Code** field, type a code that you can use later to retrieve messages from the TUI.
5. Complete the remaining fields.
6. Submit the changes.

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, enter **`save translation`**.
The system saves the translations.

Administering the Switch Link

Procedure

1. Open a Web browser and in the **Address** field type the IP address of the System Management Interface (SMI).
2. On the **Administration** menu, click **Messaging**.
3. Click **Switch Link Administration** > **Switch Link Admin**.
4. In the **Switch Number** field, type `1`.

5. 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

6. In the **Switch Integration Type** field, enter `SIP` as the type of integration between the Communication Manager virtual system and the Communication Manager Messaging virtual system.
7. In the **Transport Method** field, enter either `TCP` or `TLS` depending on the method you selected while administering the signaling group.
8. In the **Far-end Connections** field, by default only one procr connection is supported.
9. In the **Connection 1** field, enter the IP address of procr. You also need to enter the port number that was administered on procr.
10. The **Messaging Address** field displays the IP address of Communication Manager Messaging.

    Note:

    The IP address of procr and Communication Manager Messaging is the same. Hence the port numbers must be different. For example, if the Connection 1 port number is set to 5060, you can set the Messaging Address port number to 5061. The port numbers you enter on this Web page must match the values used while administering Communication Manager.

11. In the **SIP Domain** field, enter the domain used for Communication Manager and Communication Manager Messaging while administering direct SIP integration.

    Note:

    You might want to determine the capacity for Messaging at this point. For the procedure, see Determining the capacity for Messaging on page 62.

12. In the **Messaging Ports** field, enter the number of voice ports the Communication Manager Messaging virtual system uses for mailbox connections to the Communication Manager virtual system.
13. In the **Switch Trunks** field, enter the total number of trunks for Communication Manager.
14. Click **Show Advanced Options**
    The system displays advanced options that you need to administer.
15. 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.

16. In the **UDP Port Range** field, enter a starting UDP port number for RTP. The end port number is calculated automatically.
17. If you have configured SRTP for messaging, in the **Media Encryption** field, enter the type of Secure Real-time Transport Protocol (SRTP) encryption for messaging.

    Important:

    You need to 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.
18. If you want to enable DTMF transport via SIP INFO method, in the **SIP INFO FOR DTMF** field, enter `Accept`.

    Important:

    You need to set the **DTMF over IP** field to `out-of-band`.

    Note:

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

Switch Link Admin field descriptions

Field	Settings
BASIC CONFIGURATION	
Switch Number	This field should always be set to 1 unless directed otherwise by Avaya Support.
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 system automatically populates this field with the IP address version used in the IP addresses for the signaling group.
SIP SPECIFIC CONFIGURATION	

Field	Settings
Transport Method	`TLS` or `TCP`
Far-end Connections	The number of far-end connections. By default one procr connection is supported.
Connection 1	IP address of procr and the corresponding port number.
Messaging Address	Displays Communication Manager Messaging IP address.
SIP Domain	SIP domain name. The domain name must match the domain name on the switch.
Messaging Ports	The number of call answer ports to be configured.
Switch Trunks	The number of trunks to be configured.
ADVANCED OPTIONS	
Quality of Service	The value for Call Control PHB (Per Hop Behavior) and Audio PHB. The value must be in the range of 0 to 63.
UDP Port range	Specify the starting UDP port for RTP. The system automatically calculates the end port.
Media Encryption	Specify the type of media encryption. This must match the media encryption administered on the switch.
Outcall Caller ID	Phone number and/or the display name to identify the caller for calls originated by the message server. **Note:** This field is optional. If you leave this field blank, the switch automatically determines the display information.
SIP INFO for DTMF	Select **Yes** to enable out-of-band DTMF. When you set this field to **Yes**, any digits received via rtp-payload will be ignored.
Media Encryption during CapNeg	Select use of media encryption if CapNeg is present in SDP. This field is set to **Enabled** by default. If you set it to **Disabled**, the **Media Encryption** field is set to **None** automatically.

Field	Settings
Supported Header includes "replaces"	Specify whether to include replaces in the SIP Supported headers. This field is set to **No** by default.

Restarting the messaging application

Procedure

1. Under **Utilities**, click **Stop Messaging**.
2. After the application stops, click **Start Messaging**.

Administering H.323 integration for Communication Manager

Adding a signaling group for messaging

Procedure

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

   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 window.

Add Signaling Group field descriptions

Field	Setting
Group Type	h.323
Remote Office?	n
Max number of NCA TSC	10
Max number of CA TSC	10
Trunk Group for NCA TSC	(Leave blank)
Trunk Group for Channel Selection	(Leave blank)
TSC Supplementary Service Protocol	b
Near-end Node Name	`procr` (IPv4 IP address) or `procr6` (IPv6 IP address) name of the `CLAN`, 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	1720
Far-end Listen Port	11720
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.
Calls Share IP Signaling Connection?	y
DTMF over IP	out-of-band
Enable Layer 3 Test?	y
Direct IP-IP Audio Connections?	y
IP Audio Hairpinning?	n
Interworking Message	PROGress

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 field, Far-end Network Region, defaults to 1 if a value is not specified.

The Calls Share IP Signaling Connection field is set to y so that messaging does not attempt to create a new TCP/IP connection for each call.

Note:

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

The Far-end Listen port and Near-end Listen Port have the values 11720 and 1720 respectively. This is because Communication Manager and Communication Manager Messaging share the same IP address.

Adding a trunk group

Procedure

1. At the SAT interface prompt, enter **`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. Verify the fields on page 1, page 2, page 3, and page 4 of the Trunk Group window.

Add Trunk Group Page 1 field descriptions

Important:

If you do not set the **Group Type** value to `isdn`, the system does not display some of the fields of this window.

Field	Description
Group Type	isdn
Group Name	msgserver (IPv4 IP address) or msgserver6 (IPv6 IP address)
Carrier Medium	H.323
COR	1

Field	Description
Dial Access?	y
Service Type:	tie
Outgoing Display?	n
Member Assignment Method	auto
Signaling Group	The number of the signaling group you created in the creating a signaling group procedure.

1. Enter a value in the **TAC** field.
2. Enter the number of trunks (ports) in the **Number of Members** field that is appropriate for the number of messaging mailboxes for your platform.

Note:

The TAC must start with the `Dialed String` value for the DAC you set up while setting the FACs for messaging, and include the number of the trunk group. If you use the example while setting the FACs for messaging , the **TAC** value would be 199.

Refer to the Number of Ports to Mailboxes Mapping section to determine the appropriate value.

Add Trunk Group Page 2 field descriptions

Field	Description
Supplementary Service Protocol	b
Digit Handling (in/out)	enbloc/enbloc
Format	pub-unk
Disconnect Supervision - In?	y
Out?	n

Add Trunk Group Page 3 field descriptions

Field	Setting
Send Name	n
NCA-TSC Trunk Member	1
Send Calling Number	y

Field	Setting
Format	pub-unk
Send Called/Busy/Connected Number	y

Note:

The private setting is recommended. If the private setting does not work for your site, use public, unknown, or unk-pvt. You must use AAR or ARS digit conversion for path replacement to work.

Add Trunk Group Page 4 field descriptions

Field	Setting
Path Replacement with Retention?	n
Path Replacement Method	better-route
QSIG Value-Added?	y

After you submit this form, trunk groups are dynamically assigned for all trunks.

Configuring the new signaling group for messaging

About this task

After you have created the new signaling group and trunk group for messaging, you must modify the signaling group to associate it with the new trunk group.

Procedure

1. At the SAT interface prompt, enter **`change signaling-group`** <*nnn*>, where <*nnn*> represents the number of the signaling group you created while creating a signaling group for messaging.
   The system displays the signaling-group window.
2. Set the **Trunk Group for NCA TSC** field to the number of the new trunk group.

   For example, if you created the new signaling group and the new trunk group as 99, enter 99 in this field.
3. Set the **Trunk Group for Channel Selection** field to the number of the new trunk group.

   For example, if you created the new signaling group and the new trunk group as 99, enter 99 in this field.

4. Press the key combination `Control E` to save the values set in the window.

Changing a route pattern

Procedure

1. Go to the SAT interface prompt, enter **`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 window.
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 **0 1 2 3 4 W**	y y y y y n
TSC	y
CA-TSC Request	none
ITC	rest
LAR	rehu

Note:

The **CA-TSC Request** field cannot contain a value until the **TSC** field is set to `y`.

Changing AAR analysis

Procedure

1. Enter **`change aar analysis`** <*n*>, where *n* represents the first digit of the welcome to messaging extension.
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 per 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. Submit the changes.

Changing public unknown numbering

Procedure

1. At the SAT interface prompt, enter **`change public-unknown-numbering`** <n>, where <n> is the number of digits for extensions.
   The system displays the Numbering - Public/Unknown Format window.
2. On page 1 of this window, verify that appropriate values are set.

   Important:

   You must define all of the numbers that appear as the first digits in the available extension numbers that use voice mail, and the path replacement numbers on page 8 of the change system-parameters features window.
3. Verify that the value of the **Ext Len** field is set to the number of digits for extensions. For example, if the dial plan is configured for 5-digit extensions, enter 5 in this column.
4. Verify that the value of the **Ext Code** field is the first digit or digits in the range of extensions for this site plus the path replacement numbers.
5. Verify that the value of the **Trk Grp(s)** field is the number of the new trunk group that you created while creating a trunk group for messaging.

6. Verify that the value of the **CPN Len** field is the number of digits for extensions. For example, if the dial plan is configured for 5-digit extensions, enter 5 in this column.
7. Press the key combination `Control E` to save the values set in this window.

Creating a hunt group for messaging

Procedure

1. At the SAT interface prompt, enter **`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. It is only used for messaging.

   The system displays the Hunt Group window.
2. Verify that the **Group Name** field is set to `msgserver` for IPv4 IP addresses or `msgserver6` for IPv6 IP addresses.
3. Verify that the **Group Extension** field is within the range of extensions you defined, and that it is not to be used as a station or any other entity.

   This field identifies the default voice mail extension.
4. Verify that the **Group Type** is set to `ucd-mia`.
5. Verify that the **COR** field is set to `1`.

   Note:

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

   Important:

   Set the Message Center to the value `qsig-mwi`. This value is required for other fields to display on this page.
7. Verify that the **Message Center** field is set to `qsig-mwi`.
8. Verify that the **Send Reroute Request** field is set to `y`.
9. Verify that the **Voice Mail Number** field is set to the default voice mail extension.
10. 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 Communication Manager.

11. Press the key combination `Control E` to save the values in the window.

Adding a coverage path for messaging

Procedure

1. At the SAT interface prompt, enter **`add coverage path`** <*nnn*>, where <*nnn*> represents the number of a new, unused coverage path. You can substitute <*nnn*> with 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 window.
2. In the Point1 field, enter **`h`***xx*, where *xx* is the hunt group you created for messaging.

   For example, h3 represents hunt group 3.
3. Press the key combination `Control E` to save the values in the window.

Creating stations and assigning coverage paths

About this task

You must create stations so that calls can be redirected to messaging through the correct coverage path. You must create two stations to perform the initial testing of your messaging deployment.

Procedure

1. At the SAT interface prompt, enter **`add station`** <*nnn*>, where <*nnn*> represents the number of the extension that you want to create. This number must be within the range of extensions defined for this call center.
   The system displays the Add station window.
2. Enter the appropriate information in the **Type** and **Port** fields.

   Note:

   If you are unsure about what information to put in these fields, see the Completing the station screens section in the *Administrator Guide for Avaya Communication Manager* book.
3. Ensure that the **Coverage Path 1** field is set to the number of the coverage path that you created while adding a coverage path for messaging.
4. Go to page 2.

5. Verify that the **LWC Reception** field is set to `spe`.
6. Verify that the **LWC Activation?** field is set to *y*.
7. Verify that the **MWI Served User Type** field is set to `qsig-mwi`.
8. Press the key combination `Control E` to save the values in the window.

Administering the Switch Link

Procedure

1. On the navigation pane, under **Switch Link Administration**, click **Switch Link Admin**..
2. In the **Switch Number** field, type `1`.
3. 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
4. In the **Switch Integration Type** field, enter H.323 as the type of integration between the Communication Manager virtual system and the Communication Manager Messaging virtual system.
5. In the **IP Address Version** field, select **IPv4** or **IPv6**.
6. In the **Link Addresses** > **Switch** field, type the IP address of the Communication Manager virtual system.
7. In the **Messaging Ports** field, enter the number of voice ports the messaging virtual system uses for mailbox connections to the Communication Manager virtual system.
8. In the **Switch Trunks** > **Total** field, enter the value of the total switch trunks for Communication Manager.

   Note:

   You might want to determine the capacity for Messaging at this point. For the procedure, see *Implementing Avaya Aura®Communication Manager Messaging*.
9. In the **Signal Group 1** field, enter the value of the Messaging TCP port as 11720 and the Switch TCP port as 1720. The port numbers have to be different because Communication Manager and Communication Manager Messaging share the same IP address.

10. Click **Show Advanced Options**
    The system displays advanced options that you need to administer.
11. 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.
12. In the **UDP Port Range** field, enter a starting UDP port number for RTP. The end port number is calculated automatically.
13. If you have configured SRTP for messaging, in the **Media Encryption** field, enter the type of Secure Real-time Transport Protocol (SRTP) encryption for messaging.

    Important:

    You need to 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.
14. Type the **Passphrase**. This must match the Passphrase administered on the Communication Manager. This field is optional and is to be used only if SRTP encryption has been set on Communication Manager.
15. Click **Save**.
    The system calculates the number transfer ports and displays them in the **Transfer Ports** field.

    Note:

    The number of the H.323 trunks set on the Communication Manager virtual machine server must accommodate the sum of voice ports and transfer ports you administer on the Switch Link screen. This number of H.323 trunks for messaging is in addition to the H.323 trunks that the Communication Manager virtual machine requires for other functions, such as IP telephone connections, faxes, and other data connections throughout the network. The number of H.323 trunks on the Communication Manager virtual machine is listed in the **Maximum Number of H.323 Trunks** field, which is available on the System Parameters Customer Options SAT screen.

Determining the capacity for Messaging

Procedure

1. On the System Management Interface Web page, select **Administration** and click **Messaging**.
2. In the navigation pane, select **Switch Link Administration**.
3. Select **Switch Link Admin**.
   The system displays the Switch Link Administration screen.
4. Click **Show Capacity Calculator**.
5. Select the level of traffic for the Messaging system.
6. Perform one of the following:
   - Enter the minimum number of voice ports and click **Calculate Mailboxes** to know the number of supported mailboxes.
   - Enter the maximum number of mailboxes and click **Calculate Ports** to know the number of voice ports recommended by Avaya.

Note:

You may need to change the trunk group configuration according to the capacity determined using the capacity calculator.

Messaging Capacity Calculator field descriptions

Field	Setting
Traffic Load	Traffic load profile that best matches your needs. The available choices are: • **Light** • **Medium (default)** • **Heavy** • **Very Heavy** • **Extremely Heavy**
Minimum Number of Voice Ports	Number of call answer ports. The minimum value accepted is 2.
Maximum Number of Mailboxes	Number of mailboxes. The minimum value accepted is 2

Switch Link Admin field descriptions

Field	Setting
BASIC CONFIGURATION	
Switch Number	This field should always be set to 1 unless directed otherwise by Avaya Support.
Extension Length	`Variable` or any number between `1` to `50`. Mailbox extension length. The number must match the dial plan of the media server.
Switch Integration Type	`h.323`
IP Address Version	The system automatically populates this field with the IP address version used in the IP addresses for the signaling group.
H323 SPECIFIC CONFIGURATION	
Link Addresses	This field is read-only. The system automatically updates the **Messaging** IP field after you restart Messaging if the IP address version has changed.
Messaging Ports	The number of call answer ports to be configured.
Switch Trunks	The number of trunks to be configured.
Signaling Group 1	• **Members**: The system automatically updates this field with the value provided in the **Switch Trunk** field.
ADVANCED OPTIONS	
Quality of Service	The value for Call Control PHB (Per Hop Behavior) and Audio PHB. The value must be in the range of 0 to 63.
UDP Port range	Specify the starting UDP port for RTP. The system automatically calculates the end port.
Media Encryption	Specify the type of media encryption. This must match the media encryption administered on the switch.
Passphrase	The system automatically populates this field with the value administered on the switch.

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, enter **`save translation`**.
The system saves the translations.

Communication Manager Messaging SIP Integration through Session Manager

Overview

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.

To integrate SIP for Communication Manager Messaging you need to create trunks between Communication Manager and Session Manager. There is no need to create trunks between Communication Manager and Communication Manager Messaging. In contrast, for H.323 integration for Communication Manager Messaging you need to create trunks between Communication Manager and Communication Manager Messaging

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.

Log in to the System Manager R6.2 system

Procedure

1. Open a compatible Web browser on your computer.
2. In the **Address** field, enter the IP address of the System Manager.
3. Log in as `admin`.
   The system displays the System Manager Web interface.

Creating domains

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Domains**.
3. Click **New**.
4. Enter the domain name and notes for the new domain or sub-domain.
5. Select “sip” as the domain type from the drop-down list.
6. Click **Commit**.

Creating Locations

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Locations**.
   The Location Details screen is displayed.
3. Click **New**.
4. Enter the location name in the **Name** field.
5. Enter notes about the location, if required.
6. Enter the DPT parameters in the **Dial Plan Transparency in Survivable Mode** section.
7. Specify the parameters for the location in the **Overall Managed Bandwidth** section.
8. Specify the average bandwidth per call for the location in the **Per-Call Bandwidth Parameters** section. For more information, see CAC Administration on page 66.
9. Specify the alarm threshold percentage for audio and multimedia calls for the location in the **Alarm Threshold** section.
10. To add a location pattern, click **Add** under **Location Pattern**.
11. Enter an IP address pattern to match.
12. Enter notes about the location pattern, if required.
13. Continue clicking the **Add** button until all the required Location Pattern matching patterns have been configured.
14. Click **Commit**.

CAC Administration

CAC allows you to specify several types of limits on Locations. There is an overall limit (**Total Bandwidth**), which constrains the total bandwidth used for calls traversing the link of the location. There is also a multimedia sub-limit (**Multimedia Bandwidth**), which allows you to restrict calls that are not audio-only (such as video calls), to less than the full capacity of the location. This sub-limit can be used to prevent a few large video calls from exhausting the link and preventing audio calls from being made.

CAC also allows *per-call* parameters (**Maximum Multimedia Bandwidth**) to be specified at a location level, which caps the bandwidth allowed to a single call. This can proactively create room for more calls along a link by restricting video quality.

Each of these limits may be specified or left blank for any given location.

CAC operates by inspecting Session Description Protocol (SDP) contained in SIP messaging for calls. SDP identifies both the source of media (by IP address, which maps to Location) and the amount of bandwidth consumed. SDP manipulation is also used to reduce bandwidth consumption for limit enforcement. CAC allows the specification of default bandwidth assumptions for calls with unrecognized SDP, specified per Location (**Default Audio Bandwidth**). CAC also allows a per-Location restriction on how much a multimedia stream may have its bandwidth reduced (**Minimum Multimedia Bandwidth**) before it should be removed entirely. This can be used to require a minimum level of video quality.

CAC provides alarm notifications when the bandwidth usage of a location remains above a certain threshold for a sustained period of time. Snapshots of current usage are taken every 60 seconds, and if successive snapshots remain above the threshold, the alarm is raised until usage drops below the threshold. The number of snapshots and threshold required to raise the alarm can be administered per Location and per limit type. Real-time bandwidth usage can be requested using the Managed Bandwidth Usage page under Session Manager System Status.

Finally, two additional settings can change the way Session Manager performs Call Admission Control.

1. **Audio Calls Can Take Multimedia Bandwidth**, when unchecked, specifies that only multimedia calls will fill the **Multimedia Bandwidth** bucket, while audio-only calls will be limited to the bandwidth specified by **Total Bandwidth – Multimedia Bandwidth**. When checked (default), audio-only calls can consume all of **Total Bandwidth**, and **Multimedia Bandwidth** functions as a sub-limit for calls containing non-audio media.
2. Based on the **Ignore SDP for Call Admission Control** option in the Global Settings section on the Session Manager Administration page, all Session Manager instances interpret that all calls lack SDP. This causes every call to be regarded as an audio call using bandwidth defined as **Default Audio Bandwidth** under the originating location of the call.
    - This setting can be used to transform CAC into a call count enforcer. Because each call is counted equally, the limit enforced is a limit on the number of calls allowed to or from a location. By assigning SIP entities to unique locations, you can limit the number of calls to or from an entity.
    - When changing this setting, be aware that all location limits apply after different amounts of call traffic than previously, due to the change in how bandwidth for all calls is counted by CAC.
    - Session Manager 6.0 always ignores SDP. When upgrading System Manager from 6.0 to later versions, this behavior will be preserved. Otherwise, this option is disabled by default.

Creating Adaptations

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Adaptations**.
   System Manager displays the Adaptation page.
3. Click **New**. The Adaptation Details page is displayed.
4. Enter the Name, Adaptation Module, and any other required fields in the first section.
   a. Enter a descriptive name for the adaptation.
   b. Specify an adaptation module.
      - **Module name** This field contains only the name.
      - **Module parameter** field contain either a single parameter or a list of `name=value name=value name=value`.

        Note:

        The list is separated by spaces and not by commas
   c. Enter a list of URI parameters to append to the Request-URI on egress in the **Egress URI Parameters** field.

      URI parameters can be added to the Request-URI. For example, the parameter `user=phone` can be appended for all INVITEs routing to a particular SIP entity. The egress Request-URI parameters are administered from the Adaptation Details using the Egress URI Parameters field.

      The field's format is the string that should be appended to the Request URI. The string must conform to the augmented BNF defined for the SIP Request URI in RFC3261. A leading ';' is optional. Entry `;user=phone;custApp=1` is equivalent to `user=phone;custApp=1`.
   d. Enter description about the adaptation module in the **Notes** field.
5. Click **Add** under Digit Conversion for Incoming Calls if you need to configure ingress digit conversion. Ingress adaptation is used to administer digit manipulation for calls coming into the Session Manager instance.
6. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
7. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

   The minimum value can be 1. The maximum value can be 36.

8. Add **Phone Context** as an optional parameter for the ingress adaptation rules.
9. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
10. Enter the digits that you want inserted before the number in the **Insert Digits** field.
11. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.
12. Enter any additional or special adaptation data in **Adaptation Data** field.

    The adaptation data can be up to 20 characters in length with valid character values including numeric characters 0-9, +, *, #, and -.
13. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
14. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.
15. Click **Add** under **Digit Conversion for Outgoing Calls** if you need to configure egress digit conversion. Egress adaptation administers digit manipulation for calls going out of the Session Manager instance.
16. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
17. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

    The minimum value can be 1 or more. The maximum value can be 36.
18. Add **Phone Context** as an optional parameter for the egress adaptation rules.
19. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
20. Enter the digits that you want inserted before the number in the **Insert Digits** field.
21. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.
22. Enter any additional or special adaptation data in **Adaptation Data** field.

    The adaptation data can be up to 20 characters in length with valid character values including numeric characters 0-9, +, *, #, and -.

> **Note:**
> In the case of the Verizon Unscreened ANI feature, the data entered in the outgoing *Adaptation Data* field is verified to ensure that it complies with the required format of a Screened Telephone Number (STN).

23. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
24. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
25. Click **Commit**.

Create SIP entities

About Entity Links

Using Session Manager, you can create an entity link between Session Manager and any other administered SIP entity. You must configure an entity link between Session Manager and any entity that you have administered, if you need Session Manager to be able to send or receive messages from that entity directly. To communicate with other SIP entities, each Session Manager instance must identify the port and the transport protocol of its entity link to these SIP entities, in the network. Session Manager does not need to identify the port and transport protocol if the **Override Port & Transport** check box is selected on the SIP entity. Port and transport must be administered even if the **Override Port & Transport** check box is selected on the SIP entity, although these values are not used.

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

Salient features are:

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

SIP entity overview

SIP entities are elements that define each entity. You require entities that need to be linked. For SIP integration, you must create SIP entities for Communication Manager Messaging and Communication Manager Feature Server / Communication Manager Evolution Server. Session Manager uses the entity links to establish call flow between SIP endpoints and Communication Manager.

You must follow the procedure to create SIP entities to:

- 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

About this task

To administer minimal routing using Session Manager, you need to configure a SIP entity of type Communication Manager and a second SIP entity of type Session Manager. Use the SIP entities screen to create SIP entities.

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **SIP Entities**.
3. Click **New**.
4. In the **Name** field, enter the Name of the SIP entity .
5. Enter the FQDN or IP address of the SIP entity in the **FQDN** or **IP Address** field.
6. Select the type of SIP entity from the drop-down menu in the **Type** field.

   For SIP entity type *Session Manager* follow the instructions as follows and for non-Session Manager type SIP entity, see the related field description topic for details.
7. If you need to specify the location for the SIP entity, in the **Location** field, click a location.
8. If the SIP entity Type is *Session Manager* and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** field.

   In cases when Session Manager cannot associate any administered routing policies, then the request is sent to the SIP entity administered as an outbound proxy. If no outbound proxy is provisioned, then Session Manager will proxy the request on its own.
9. Enter a regular expression string in the **Credential name** field. The Credential name is used for TLS connection validation by searching for this string in the SIP entity identity certificate.

- If you do not need to perform the additional validation on the SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
- If you need to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax.
- If you need to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax.

Note:

IP Address is searched by default when any string is configured in the Credential Name.

The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some examples:

For `www.sipentity.domain.com`, use the string `www\.sipentity\.domain\.com`.

For `192.14.11.22`, use string `192\.14\.11\.22`. You can look for a subset of the string or you can create a wild card search. For example, to look for `domain.com` as a substring, use the string `domain\.com`.

10. For non-Session Manager type of SIP Entity, enter the Loop Detection parameters.
11. In SIP Link Monitoring, use the drop-down menu to select one of the following:
    - Use Session Manager Configuration: Use the settings in **Session Manager** > **Session Manager Administration**
    - Link Monitoring Enabled: Enables link monitoring on this SIP entity.
    - Link Monitoring Disabled: Link monitoring will be turn off for this SIP entity.
12. If you need to specify the Entity Links, click **Add**.
13. In the **Name** field, enter the name.
14. From the drop-down list, enter the SIP entity 1 by selecting the required **Session Manager** SIP entity 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.
15. Enter the SIP entity 2 by selecting the required non-Session Manager SIP entity from the drop-down list box 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.

16. Select the Connection Policy for the link using the **Connection Policy** drop-down list box. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
17. Select the **Deny New Service** checkbox to deny any service for the associated entity link.
18. If you need to specify the Port parameters, click **Add** in Port section. When Session Manager receives a request where the host-part of the request-URI is the IP address of Session Manager, it associates one of the administered domains with the port on which the request was received. Add Failover ports if the SIP entity is a failover group member. For details, see *Failover Groups* section.
19. Enter the necessary Port and Protocol parameters.
20. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.
21. Add and remove SIP Response Codes and Reason phrases to OPTIONS requests to mark the SIP entity is up or down.
22. Click **Commit**.

Create Entity Links

Entity links overview

Note:

It is assumed that you have created an entity for Session Manager in System Manager.

Entity link between Session Manager and other SIP entities.

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

Note:

If you are administering SIP for Communication Manager Messaging Embedded, ensure that the Communication Manager and Communication Manager Messaging ports they listen to are different since they use the same IP address. However, for Communication Manager Messaging Federal you could use the default ports for Communication Manager and Communication Manager Messaging since they use different IP addresses.

Important:

While creating entities, if you enter the protocol as**TLS** or **TCP**:

- Enter the port number for Communication Manager Feature Server as 5060 / 5061.

  or Enter the port number for Communication Manager Evolution Server as 5070/ 5071.
- Enter the port number for Communication Manager Messaging as 6060 / 6061.

Creating Entity Links

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Entity Links**.
3. Click **New**.
4. Enter the name in the **Name** field.
5. 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 an Session Manager instance.

   The default port for TCP and UDP is 5060. The default port for TLS is 5061.
6. 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.
7. Select the connection policy for the link using the **Connection Policy** drop down list. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities. There are three choices
   - Trusted.
   - Trusted HA: Connection policy for high availability clustered hosts such as Avaya Aura® Contact Center. It is identical to the “Trusted” Connection Policy except that the TCP Keep Alive window value is 3 seconds.
   - Untrusted.
8. Click **Commit**.

Creating Time Ranges

About this task

You can use the Time Ranges screen to administer time ranges with start and end times.

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Time Ranges**.
3. Click **New**.
4. Enter the name, 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.
5. 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 System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Routing Policies**.
3. To add a new routing policy, click **New**.
4. Under the General section, enter a routing policy name and notes in the relevant fields.
5. In **Retries** field, enter the number of retries for the destination SIP entity.

Note:

- The default value in **Retries** field is zero, and the valid values are 0-5.
- Select the **Disabled** check box to disable the routing policy.

During conditions when Session Manager sends an Invite to the Avaya Aura® Contact Center (AACC) that has failed, one of two things can happen:

a. The AACC does not respond at all which is a "passive failure".

b. The AACC responds with an "active failure".

In either case, Session Manager attempts to resend the initial Invite up to Retries times. This allows time for the AACC standby server to take control and successfully process the call setup.

- For a passive failure, the time between retries is the value of Timer B/F (which is configured for each Entity).
- For an active failure, the time between retries is the value of Timer B/F divided by the configured number of Retries.

6. Under the SIP Entities 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 press **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. Enter the relative Rankings that you would like associated 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. Under the Dial Patterns and Regular Expressions sections, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy.

14. Select a dial pattern from the pattern list or a regular expression from the regular expression list, and click **Select**.
15. 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 starting and ending mailbox extensions.
- 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 starting and ending mailbox extensions.
- Enter the dial pattern.
- 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

About this task

The Dial Patterns screen is used to create Dial Patterns and associate the Dial Patterns to a Routing Policy and Locations.

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Dial Patterns**.
3. Click **New**. The Dial Pattern Details screen is displayed.
4. Enter the Dial Pattern General information in the General section. Note that a Domain can be provided to restrict the Dial Pattern to the specified Domain.
5. Click **Add** under the Originating Locations and Routing Policies section.
6. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
7. Click **Select** to indicate that you have completed your selections.
8. If you need to specify that calls from the specified locations will be denied, click **Add** under the Denied Locations section.
9. Select all the Locations that are to be denied and click **Select** to indicate that you have completed your selections.
10. Click **Commit**.

    Note:

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

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

About this task

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 System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Regular Expressions**.
3. Click **New**. The Regular Expression Details screen is displayed.
4. Enter the regular expression pattern in the **Pattern** field.
5. Specify a rank order for the regular expression. A lower rank order indicates a higher priority.
6. To deny routing for a matched regular expression pattern, select the **Deny** check box.
7. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
8. Select the required routing policies that you want associated with the Regular Expression by selecting the respective check boxes.
9. Click **Select** to indicate that you have completed your selections.
10. To remove an associated routing policy, select the routing policy and click **Remove**.
11. 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:
    a. Log in as `init`
    b. 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.

Adding privileged administrator login

Procedure

1. Log in to the System Management Interface Web page.
2. On the **Administration** menu in the top horizontal bar, click **Server (Maintenance)**.
3. Click **Security > Administrative Accounts**.
4. Under **Select Action**, select **Add Login**.
5. Select **Privileged Administrator**
6. Click **Submit**.
7. Fill in all the fields that define the privileged administrator user.
8. Click **Submit**.

Administrator Accounts field descriptions

Field descriptions

Name	Description
Add Login	Enables you to add a user ID for one of the following profiles: • Privileged Administrator • Unprivileged Administrator • SAT Access Only • Web Access Only • Modem Access Only • CM Messaging Access Only • Avaya Partner Login (dadmin)

Name	Description
	• Avaya Partner Craft Login • Custom Login
Change Login	Enables you to change the user profile of the selected user ID.
Remove Login	Enables you to remove the user profile of the selected user ID.
Lock/Unlock Login	Enables you to lock or unlock the selected user ID.
Add Group	Enables you to add a user group.
Remove Group	Enables you to remove the selected user group.

Button descriptions

Name	Description
Submit	Performs the selected action such as adding a user profile.

Add Login field descriptions

Field descriptions

Name	Description
Login name	Is the user ID of the user whose profile is being created or edited.
Primary group	Is the primary group to which the user belongs.
Linux shell	Is the full path of the shell script filename that is executed when this user logs on.
Home directory	Is the home directory of the user.
Lock this account	Indicates whether the user has been locked or not. When this check box is selected, the user is not allowed to log on to Communication Manager System Management Interface. **Note:** This feature helps you to create an ID for a user before the user starts using it.
Date after which account is disabled	Is the date in YYYY-MM-DD format. After this date, the user cannot log in to

Name	Description
	Communication Manager System Management Interface.
Select type of authentication	Denotes the type of authentication to be used when the user attempts to log on to Communication Manager System Management Interface. The following are the types of authentication available: 1. Password: The user enters a password, which is validated against the one existing in the system. 2. ASG: enter key: The user enters the ASG key, which is validated against the one existing in the system. 3. ASG: Auto-generate key: The user enters the auto-generated ASG key.
Enter password or key	Is the user password or the ASG key to be stored in the system. This is used to validate the user input of password or ASG key at the time of login.
Re-enter password or key	Is the user password or the ASG key that must be entered exactly in the same way as was entered for the **Enter password or key** field.
Force password/key change on next login	Indicates whether or not the user must be forced to change the password or the ASG key when the user tries to log in for the first time. If you select **Yes**, the user has to change the password or the key at the time of first login.

Button descriptions

Name	Description
Submit	Accepts the changes and adds a user profile in the 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, enter **`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 **Service Type** field to `tie`.
3. On page 3, set the **Numbering Format** field to `public`.
4. On page 4, set the **Convert 180 to 183 for Early Media?** field to `n`.
5. Press `Control E` to 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, enter `add signaling-group` <*nnn*>, where <*nnn*> represents the number of the new signaling group.
2. Press `Enter`.

   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 window.
3. Set the value of the **Group Type** field to `SIP`.
4. Set the value of the **Transport Method** field to the value you set for the **Protocol** field while administering Session Manager.
5. Set the value of the **IMS 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. Press Control E to 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, enter `add signaling-group` <*nnn*>, where <*nnn*> represents the number of the new signaling group.
2. Press `Enter`.

   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 window.
3. Set the value of the **Group Type** field to `SIP`.
4. Set the value of the **Transport Method** field to the value you set for the **Protocol** field while administering Session Manager.
5. Set the value of the **IMS Enabled?** field to `n`.
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. Press Control E to save the changes.

Next steps

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

Changing IP network region

Procedure

1. At the SAT interface prompt, enter `change ip-network-region` <*n*>, where <*n*> represents the value in the **Far-end Network Region** field.
2. Press `Enter`.
   The system displays the IP Network Region page.
3. Set the value of the **Authoritative Domain** field to the SIP domain name.
4. On Page 4, in the **Codec set** column, type `1`.
5. In the **AGL** column, type `ALL`.
6. Save the changes.

Enable fax

About this task

It is optional to enable fax.

Procedure

1. At the SAT interface prompt, enter `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, enter **`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. It is only used for messaging.

   The system displays the Hunt Group window.
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. Press the key combination `Control E` to save the values in the window.

Create a route pattern for the new trunk group

Changing a route pattern

About this task

Important:

The route pattern must point to the SIP trunk between Communication Manager and Communication Manager Messaging.

Procedure

1. Go to the SAT interface prompt, enter **`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 window.
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 between Communication Manager Feature Server/ Evolution Server and Session Manager.
FRL	0
DCS/ QSIG Intw	n
IXC	user
BCC VALUE **0 1 2 3 4 W**	y y y y y n
TSC	y
CA-TSC Request	none
ITC	rest
LAR	rehu

Note:

The **CA-TSC Request** field cannot contain a value until the **TSC** field is set to `y`.

Changing AAR analysis

Procedure

1. Enter **`change aar analysis`** <*n*>, where *n* represents the first digit of the welcome to messaging extension.
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 per 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. Submit the changes.

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 between Communication Manager Feature Server/ Evolution Server and Session Manager.
FRL	0
DCS/ QSIG Intw	n
IXC	user
BCC VALUE 0 1 2 3 4 W	y y y y y n
TSC	y
CA-TSC Request	none
ITC	rest
LAR	rehu

Note:

The **CA-TSC Request** field cannot contain a value until the **TSC** field is set to `y`.

Communication Manager Messaging administration

Administering the Switch Link

Procedure

1. On the navigation pane, select **Switch Link Administration**.
2. Click **Switch Link Admin**.
   The system displays the Switch Link Administration screen.
3. In the **Switch Number** field, type `1`.
4. In the **Extension Length** field, enter the appropriate length.

   Starting with 6.2, CM Messaging allows you to set extensions up to 50 digits.
5. In the **Switch Integration Type** field, select `SIP` as the type of integration between the Communication Manager virtual system and the messaging virtual system.
6. 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 ra nge 0 to 63. The value must match the corresponding number configured for the network region used by the messaging signaling group on the switch.
7. In the **Transport Method** field, select either `TCP` or `TLS` depending on the method you selected while administering Session Manager.
8. In the **Far-end Connections** field, enter 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 enter the IP addresses of Session Manager.

   Note:

   Communication Manager Messaging supports up to 12 connections.
9. In the **Connection 1** field, enter the Asset IP address of Session Manager. You also need to enter the port number that was administered on Session Manager for the entity link.
10. The **Messaging Address** field, displays the IP address of Communication Manager Messaging. You also need to enter the port number that was administered on Session Manager for the entity link.
11. In the **SIP Domain** field, enter the domain used for Communication Manager and Communication Manager Messaging while administering Session Manager.

12. In the **Messaging Ports** field, enter the number of voice ports the messaging virtual system uses for mailbox connections to the Communication Manager virtual system.
13. In the **Switch Trunks** field, enter the total number of trunks for Communication Manager.
14. If you have configured SRTP for messaging, in the **Media Encryption** field, enter the type of Secure Real-time Transport Protocol (SRTP) encryption for messaging.

    Important:

    You need to 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. In the **SIP INFO for DTMF** field, enter `Accept` to receive digits from SIP INFO

    Note:

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

    Important:

    You need to set the **DTMF over IP** field to `out-of-band`.
16. Click **Save**.

Chapter 5: Administering Communication Manager Messaging

Enabling messaging

Procedure

1. Open a compatible Web browser.
2. In the **Address (or Location)** field, type the IP address or name of the virtual system and press **Enter**. For example, http://serverIPaddress.com.
3. Log in as craft.
   The system displays the System Management Interface Web page
4. Click **Administration** > **Server (Maintenance)**.
5. Click **Miscellaneous** > **Messaging Software**.
6. Click **Enable**.

Obtaining language files for Communication Manager Messaging

About this task

You might need one or more remote field update (RFU) files. If the Messaging application uses optional languages, obtain the corresponding data files.

Procedure

1. On the Avaya Support Web site, in the navigation pane, click **Downloads**.
2. Enter the name of the product as Communication Manager Messaging.
3. Press **Enter**.
   The System displays a list of available downloads.

4. Download the file(s).

Patch management

Patch installation overview

A Service Pack provides product updates and bug fixes. When a Service Pack is available on the Avaya Support website, the supporting information clearly states the issues addressed in the Service Pack. Even if you do not have problems, implement the Service Packs to keep the systems up-to-date and minimize the likelihood of future issues.

A patch provides critical security, performance, and stability fixes or updates. A Service Pack is a bundle of updates, fixes, enhancements, and previously released patches. In this document, the word *patches* refers to both patches and Service Packs.

You can install, download, and manage the patches from the System Platform Web Console.

You must install the following patches in addition to the currently installed software:

- Communication Manager: You must install Communication Manager patches because Communication Manager Messaging uses the Communication Manager platform that requires software updates.
- Communication Manager Messaging

You must install the following patches when available:

- Security
- Kernel

> **Important:**
> Install kernel updates only during a planned downtime for system maintenance.

To download the latest patches and to obtain the necessary information, see *Avaya Aura® Messaging Release Notes* on the Avaya Support website at https://support.avaya.com/Products/P0792.

> **Important:**
> Before you apply a patch, back up the system. When you install the latest patch, the installation program automatically uninstalls the previous patch. So if you remove a patch, the removal does not reinstall the previous patch or revert the system to the previous state,

that is, the state before the patch was installed. To revert the system to the previous state, you must reinstall the previous patch.

For more information, see the “Backup and restore” section of *Administering Avaya Aura® Messaging*.

Caution:

Patch installation process affects the availability of the Messaging service.

Installing patches

Before you begin

Ensure that the Messaging system is running.

Procedure

1. Log on to the System Platform Web Console.
2. Click **Server Management** > **Patch Management** > **Download/Upload**.
   The system displays the Search Local and Remote Patch page.
3. From the **Choose Media** drop-down list, select the medium to search for a patch.
   The following table lists the available options.

Option	Action
Avaya Downloads (PLDS)	Provide **SSO Login** and **SSO Password** and then click **Search**. **Note:** This option is not available for Avaya Services.
HTTP	Specify the **Patch URL** and click **Search**. If the patches are located on a different server, you might have to configure a proxy depending on your network. Click **Configure Proxy** to specify a proxy server if required.
SP Server	Specify the **Patch URL** and click **Search**. **Note:** This option is not available for Avaya Services.
SP CD/DVD	Click **Search**.
SP USB Disk	Click **Search**.
Local File System	Click **Add** to locate the patch file on your computer and then click **Upload**.

For more information, see Search Local and Remote Patch field descriptions on page 24.

The system displays the Select Patches page.

4. From the **Select Patches** list, select the patch that you want to download.
5. Click **Select**.
The system displays the Patch Detail page.
6. On the Patch Detail page, click **Install**.
For more information, see Patch Detail field descriptions on page 26.
The Patch Detail page displays the progress of the patch installation process.

Next steps

Verify the patch installation.

Search Local and Remote Patch field descriptions

Name	Description
Supported Patch File Extensions	The patch that you select for installing. Ensure that the patch matches the extensions in this list. For example, *.tar.gz,*.tar.bz,*.gz,*.bz,*.zip,*.tar,*.jar,*.rpm,*.patch.
Choose Media	The media options from where you can search for a patch The available options are: • **Avaya Downloads (PLDS)** Download the patch files located on the Avaya Product Licensing and Delivery System (PLDS) website, you must enter an Avaya SSO login and password to access this site. The list on this site contains all the templates that your company is entitled to. Each line in the list begins with the sold-to number. Use the sold-to number to select the appropriate template for your site. For more information about a sold-to number, hold the mouse pointer over the number. • **HTTP** Download the patch files located on an HTTP server, you must enter the patch location information. • **SP Server**:

Name	Description
	Download the patch files located in the `/vsp-template` directory in the Console Domain of the System Platform server, you must specify the patch location for the server. **Tip:** When you move files from a laptop to the System Platform Server, you may encounter some errors, as System Domain (Dom–0) and Console Domain support only SCP. Most laptops do not support SCP. To enable SCP, download the following two programs: - Pscp.exe - WinSCP For detailed procedures on how to download the programs, search the Internet. • **SP CD/DVD** Download the patch files located on a CD-ROM or DVD in the CD/DVD drive on the System Platform server. • **SP USB Disk** Download the patch files located on a USB flash drive connected to the server. • **Local File System** Download the patch files located in a local file system.
SSO Login	The log-in ID to log on to Single Sign On. The system activates this field only when you select the **Avaya Downloads (PLDS)** option to search for a patch.
SSO Password	The password for Single Sign On. The system activates this field only when you select the **Avaya Downloads (PLDS)** option to search for a patch.
Patch URL	The URL of the server where the template files are located. The system activates this field only when you select the **HTTP** or **SP Server** option to search for a patch.

Patch Detail field descriptions

Name	Description
ID	The file name of the patch file.
Version	The version of the patch file.
Product ID	The name of the virtual machine.
Description	The short description of the patch file.
Detail	The virtual machine name for which the patch is applicable. This field is not applicable for Communication Manager Messaging patches.
Dependency	The dependency that the patch file might have on any other file, if any. This field is not applicable for Communication Manager Messaging patches.
Applicable for	The software load for which the patch is applicable. This field is not applicable for Communication Manager Messaging patches.
Service effecting when	The action (if any) that causes the selected patch to restart the Communication Manager Messaging services.
Restart this console when	The conditions or circumstances when the System Platform Web Console must be restarted. This field is not applicable for Communication Manager Messaging patches.
Disable sanity when	The stage at which the condition is set to disable. This field is not applicable for Communication Manager Messaging patches.
Status	The status to show whether the patch is available for installation or already installed.
Patch File	The path where the patch is cached on the Console Domain.

Verifying the patch installation

Procedure

1. Click **Server Management** > **Patch Management** > **Manage**.
   The system displays the Patch List page.
2. Verify that the patches you installed (Communication Manager Messaging and Communication Manager) are displayed under the *cmm* heading and the status of the patch is **Active**.
   For more information, see Patch List field descriptions on page 27.

Patch List field descriptions

The Patch List page displays the patches on the System Platform server for installation or removal. To view the details of the patch file, click the file name.

Name	Description
System Platform	Lists the patches available for System Platform.
Solution Template	Lists the patches available for the respective solution templates.
cmm	Lists the patches available for Communication Manager Messaging.
Patch ID	Lists the file name of a patch.
Description	Provides information on a patch. For example, describes a patch available for System Platform as: SP patch.
Status	Shows the status of a patch. The possible values of **Status** are **Active** and **Not Installed**.
Service Effecting	Shows if installing the patch causes the Communication Manager Messaging virtual machine to reboot.

Removing patches

Procedure

1. Click **Server Management** > **Patch Management** > **Manage**.
   The Patch List page displays the list of patches and the current status of the patches.
2. On the Patch List page, click a patch that you want to remove.
3. On the Patch Detail page, you can:
   - Click **Remove** to uninstall the patch.
   - Click **Remove Patch File** to clean up the hard disk drive by deleting the installation file for an uninstalled patch.

Restarting the messaging application

Procedure

1. Under **Utilities**, click **Stop Messaging**.
2. After the application stops, click **Start Messaging**.

Setting Communication Manager Messaging server parameters

Procedure

1. Select **Server Administration**.
2. Select **Messaging Server Admin**.
   The system displays the Edit Messaging Server screen.
3. In the **Server Name** field, type the name of the voice mail system. This name must match the name in the **Host Name** field that you entered in the Template Details screen while installing Communication Manager Messaging.

4. In the **Password** field, type a password for other messaging servers to use to access this messaging server. The customer provides this password.
5. In the **Starting Extension** and **Ending Extension** fields of the ADDRESS RANGES table, enter the starting and ending extensions that are assigned to this call center.

   Note:

   You can setup variable extensions in R6.2. **Starting Extension** and **Ending Extension** lengths must be same while administering variable length extensions.
6. Verify that the **IP address** field contains the IP address of the Communication Manager Messaging virtual machine.
7. Verify that the **Server Type** field is set to `TCP/IP`.
8. Verify that the **Voiced Name?** field is set to `NO`.
9. Verify that the **Extension Length** field is set to the value used in the dial plan for this site.
10. Verify that the **Voice ID** is set to `0`.
11. Verify that the **Default Community** is set to `1`.
12. Click **Save**.
    The system displays the message `Server information modified successfully`.

Setting system-wide Messaging parameters

Procedure

1. Select **Messaging Administration** > **System Administration**.
   The system displays the Administer System Attributes and Features screen.
2. In the **Lock Duration** field, type the length of time a mailbox remains locked after the administered number of failed login attempts.
3. In the **Consecutive Invalid Attempts** field, type the number of login attempts allowed before a mailbox is locked.
4. In the **Minimum Password length** field, type the minimum number of digits that subscriber passwords must contain.
5. In the **Passwords History** field, type the number of old passwords that the system saves to check against old password reuse by a subscriber.

6. 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.
7. 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. For the procedure, see Creating stations and assigning coverage paths. 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. In the navigation pane, select **Messaging Administration** > **Subscriber Management**.
   The system displays the Manage Subscribers screen.
2. In the **Local Subscriber Mailbox Number** field, type the extension number of the first test subscriber.
3. Click **Add** or **Edit**.
   The system displays the Add Local Subscriber screen.
4. In the **Name** field, type the name of the first test subscriber.
5. In the **Password** field, type the password for the subscriber's mailbox.
6. Ensure that the **Switch Number** field displays the number you administered in the **Switch Number** field on the Switch Link Administration screen.
7. Click **Save**.
8. Repeat Step 2 through Step 7 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 access messaging

Before you begin

Refer to the Creating stations and assigning coverage paths section and note down a station number.

Refer to the Creating a trunk group for messaging section and note down the messaging hunt group number.

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 by reviewing the previous procedures in this document.

Calling an extension to verify messaging coverage

Procedure

1. Call one of the two stations that you set as a subscriber to the messaging server.
2. Do not let the call be answered.
   You should be routed to the messaging system. You hear the greeting, `Your call is being answered by AUDIX`. If you do not hear this greeting, ensure that the settings for the hunt group, coverage path, station, and subscriber are set properly by reviewing the configuration procedures in this document.
3. Leave a message and verify that the Message Waiting Indicator (MWI) lamp on the receiving extension is lit.
4. From the receiving extension, retrieve the message and verify that the MWI lamp is no longer lit.

Index