Implementing Avaya Aura™ Communication Manager Messaging

Release 6.0
18-603644
June 2010

Notices

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 Web sites 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 Web site: 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.

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 End User a license within the scope of the license types described below. 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 End User. “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. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified 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 communicate 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 by Avaya 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). End User 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). Customer 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”). (see “Third-party Components” for more information).

Copyright

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

Third-party components

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

Trademarks

Downloading Documentation

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

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: 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, or S8510 Server. 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 or an S8510 Server
- Embedded Survivable Core on an S8300D Server

IPv6 support

The IPv6 addressing administration provided in this offer is only intended for Government Solutions accounts which require IPv6 addressing and connectivity for specific requirement mandates. It is not intended for implementation in commercial market solutions. In general, customers should continue to administer IPv4 addressing.

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 3.4x10^{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 4.3x10^{9}	128-bit, about 3.4x10^{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. See to the detailed feature information and Branch Gateway features

Prerequisite

License file installation

Communication Manager Messaging needs a separate license file for its features to be functional. You install the license before installation of the Communication Manager template.

Chapter 2: Administering Communication Manager for Communication Manager Messaging

Communication Manager installation

Install and configure Communication Manager.

Refer to the *Installing and Configuring Avaya Aura™ Communication Manager*, Release 6.0 for more information.

Accessing the Messaging virtual machine

Using the SSH connection type

Prerequisites

PuTTy to access the virtual system.

1. Open an instance of 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.

Related topics:

Logging in to the virtual system on page 12

Logging in to the virtual system

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

You can access the System Management Interface (SMI) either 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.

1. Open a compatible Web browser.

   Currently, SMI supports only Microsoft Internet Explorer 7.0.
2. Depending on the server configuration, choose one of the following:
   - LAN access by IP address

     If you log on to the corporate local area network, type the unique IP address of the S8xxx Server in 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 has been administered with the host name, type the host name, such as `http://media-server1.mycompany.com`.
   - Portable computer access by IP address

     If you 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 is generated by the Logon page. 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 Communication Manager System Management Interface home page.

Administering Communication Manager for Communication Manager Messaging

Connecting to the Communication Manager server SAT interface

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

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

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, you must contact your project manager to have a new license file, with the proper features, regenerated for this installation. You cannot perform the installation without the proper customer options. If you do not have the correct options, contact your project manager or the Avaya support representative.

Note:

Press the key combination `Control N` to navigate to the next screen and the `Control P` keys to go back to a previous screen on the SAT interface.

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

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.

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

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 an Enterprise Survivable Server (ESS) is being used for reliability. An ESS 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.

Related topics:

Feature-Related System Parameters window field descriptions on page 17

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.

Parameter name	Description
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.
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.

Related topics:

Defining IP interfaces for Processor Ethernet on page 18

Defining IP interfaces for Processor Ethernet

1. Enter **`change ip-interfaces procr`**.

The system displays the IP Interfaces window.

2. Enter values for the fields in the window.

Related topics:

IP interfaces field descriptions on page 19

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.

Field (Page 2)	Description
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

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

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

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.

Related topics:

Path replacement settings on page 21
Converting AAR and ARS digits on page 21

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

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

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

At the SAT interface prompt, enter **`save translation`**.
The system saves the translations.

Chapter 3: Administer H.323 or SIP switch integration

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

You can administer Communication Manager Messaging for either H.323 protocol or SIP protocol integration. SIP integration allows SIP endpoints to be registered to Session 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 only supports **rtp-payload** as the DTMF set.

Administering H.323 integration for Communication Manager Messaging

Create a signaling group for messaging

Adding a signaling group for messaging

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.

Related topics:

Add Signaling Group field descriptions on page 24

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` or name of the `CLAN`, depending on which interface connects to Communication Manager Messaging.
Far-end Node Name	Name of the messaging server 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.

Changing the IP Network Region

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 window.
3. Verify that the **Intra-region IP-IP Direct Audio** field is set to `yes`.
4. Verify that the **Inter-region IP-IP Direct Audio** field is set to `yes`.
5. Verify that the **IP Audio Hairpinning?** is set to `n`.
6. Note the value in the **Codec Set** field for use later in the procedure.
7. Go to page 3. (Key combination `Control N`)
8. Verify that the value of the **src rgn** field matches the **Far-end Network Region** value.
9. Enter the value of the **Codec Set** field you noted in step 6.
10. Press the key combination `Control E` to save the values set in the window.

Changing the IP Codec Set

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.

Create a trunk group for messaging

Adding a trunk group

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
Carrier Medium	H.323

Field	Description
COR	1
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
Format	private
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

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.

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.

Create a route pattern for the new trunk group

Changing a route pattern

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

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

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

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`.
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

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.

   Important:

   At this point, an Avaya Technician must be engaged to change the login passwords.

Creating stations and assigning coverage paths

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.

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

1. On the navigation pane, under **Switch Link Administration**, click **Switch Link Admin**..
2. In the **Switch Number** field, type `1`.
3. Select an extension length in the **Extension Length** field. 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 **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.
7. In the **Link Addresses** > **Switch** field, type the IP address of the Communication Manager virtual system.
8. In the **Link Addresses** > **Messaging** field, type the IP address of the messaging virtual system.

   Note:

   If you select IPv6, the IP address you entered in the **Link Addresses** field automatically change to IPv6 format.
9. 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.
10. In the **Switch Trunks** > **Total** field, enter the value of the total switch trunks for Communication Manager.
11. 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.
12. 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.

Note:

You also need to configure SRTP on the Communication Manager virtual system.

13. 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.
14. 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.

Related topics:

Determining the capacity for Messaging on page 34

Determining the capacity for Messaging

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.

Saving translations

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

At the SAT interface prompt, enter **`save translation`**.

The system saves the translations.

Administering the SIP Integration for Communication Manager Messaging

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 R6.0 system

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

Create a domain or set of domains if you plan to use domain-based routing.

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > **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

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > **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. Specify the parameters for the location in the **Overall Managed Bandwidth** section.
7. Specify the average bandwidth per call for the location in the **Per-Call Bandwidth Parameters** section.
8. To add a location pattern, click **Add** under **Location Pattern**.
9. Enter an IP address pattern to match.
10. Enter notes about the location pattern, if required.
11. Continue clicking the **Add** button until all the required Location Pattern matching patterns have been configured.
12. Click **Commit**.

Creating Adaptations

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Adaptations** to open 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** 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 or more. 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. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
13. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.

14. 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.
15. 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.
16. 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.
17. Add **Phone Context** as an optional parameter for the egress adaptation rules.
18. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
19. Enter the digits that you want inserted before the number in the **Insert Digits** field.
20. 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.
21. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
22. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
23. Click **Commit**.

Create SIP entities

About Entity Links

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

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

- 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

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

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

8. If you need to specify the Location for the SIP entity, click the drop-down selector for the **Location** field and select a location.
9. 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.
10. 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 want 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 want 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 want 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”
11. Under SIP Link Monitoring, use the drop-down menu to select one of the following:

    - Use Session Manager Configuration – Use the settings under **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. Enter the name in the **Name** field.
14. 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.

15. 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.

16. If the SIP entity is trusted, select the **Trusted** check box. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
17. Select the protocol you require for the link using the **Protocol** drop-down list.
18. If you need to specify the Port parameters, click **Add** under Port. When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
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. 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

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > **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. If the SIP entity is trusted, select the **Trusted** check box. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
8. Select the protocol you require for the link using the **Protocol** drop-down list.
9. Click **Commit**.

Creating Time Ranges

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

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > **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

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > **Policies**.
3. Click **New**.
4. Enter a routing policy name and notes in the relevant fields in the General section. Note that the routing policy can be disabled by selecting the **Disabled** check box.
5. Click **Select** under the SIP Entities as Destination section. This is where you can select the destination SIP entity for this routing policy.
6. Select the required destination and click **Select**.
7. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the Time of Day section.
8. Select the Time of Day patterns that you want to associate with this routing pattern and press **Select**.

   If there are gaps in the Time of Day coverage that you select, Session Manager displays a warning message. If such gaps exist in the Time of the Day coverage, randomness in routing selections may be observed

9. Enter the relative Rankings that you would like associated with each Time Range. Lower ranking values indicate higher priority.
10. Under Dial Patterns or Regular Expressions, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.

    This field can be left blank; the routing policy can be added to the dial pattern or regular expression when you add it.
11. Under Dial Patterns or Regular Expressions, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**. This field can be left blank; the routing policy can be added to the dial pattern or regular expression when you add it.
12. 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

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

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > **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

The Regular Expressions screen enables you to create regular expressions and associate them with routing policies. You cannot save a regular expression unless it has a routing policy associated to it.

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > **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

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**.

Related topics:
Administrator Accounts field descriptions on page 49
Add Login field descriptions on page 49

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) • 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.

Name	Description
	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 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

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

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

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

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

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

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

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

It is optional to enable fax.

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

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`.
3. Verify that the **Group Extension** field matches the value used in the **Pattern** field of the dial pattern created for Communication Manager Messaging while administering Session Manager. This value must be within the range of extensions you defined. Do not use the value 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 `sip-adjunct`. This value is required for other fields to display on this page.
7. Verify that the **Message Center** field is set to `sip-adjunct`.
8. Verify that the **Voice Mail Number** field is set to the default voice mail extension.
9. 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.
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 messaging.
11. 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

Important:

The route pattern must point to Session Manager.

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

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

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.
5. In the **Switch Integration Type** field, enter `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 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.
7. In the **Transport Method** field, enter 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.
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. Click **Save**.

Chapter 4: Administering Communication Manager Messaging

Enabling messaging

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**.

Editing privileged administrator login

Prerequisites

You must be logged into the System Management Interface.

1. In the menu bar, click **Administration** > **Server (Maintenance)**.
2. Click **Security > Administrator Accounts**.
3. Under **Select Action**, select **Change Login**.
4. Select **admin** from the drop-down list.
5. Click **Submit**.

6. Fill in all the fields that define the privileged administrator user.
7. Click **Submit**.

Related topics:
Administrator Accounts field descriptions on page 49
Add Login field descriptions on page 49

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) • 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 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.

Obtaining remote field updates and language files for Communication Manager Messaging

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

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**.
4. Click the **Download** tab to view the available downloads.
5. Download the file(s).

Copying files to the server

Use the Web interface of the System Management Interface to copy the latest RFUs, if any, and optional languages, if any, from the Services laptop to the virtual system. The backup tar files need to be copied from the laptop to the Messaging server.

1. Select **Administration**.
2. Click **Server (Maintenance)**.
3. In the navigation pane, select **Miscellaneous**, click **Download Files**.
4. Select one of the following:
   - **File(s) to download from the machine I'm using to connect to the server**
   - **File(s) to download from the LAN using URLs**

     Enter the name of the proxy server.

5. Click **Browse** to locate the file(s).
6. Click **Download** to copy the files to the media server.

Downloading the Communication Manager patch

1. On the System Management Web interface, click **Administration** > **Server (Maintenance)**.
2. In the **Miscellaneous** field, click **Download Files**.
3. Select one of the following methods to download the patch:
    - File(s) to download from the machine I'm using to connect to the server.
    - File(s) to download from the LAN using URL.
4. Depending on the download method you select, perform either of the following:
    - Click **Browse** to download the patch.
    - Enter the URL to download the patch and enter the host name and domain name of the proxy server.
5. Click **Download**.

Installing RFU

Perform this procedure only if Communication Manager Messaging is enabled.

Skip this procedure there are no remote field update (RFU) files on the Avaya Support site.

1. On the System Management Interface Web page, select **Administration**.
2. Click **Messaging**.
   The system displays the Messaging Administration screen.
3. In the navigation pane, under the **Software Management** section, click **Software Install**.
4. Click **Continue without current system backup**.

The system displays the Following packages will be installed... screen. The messaging RFUs are listed on the screen.

5. Click **Installed selected packages**.

   Important:

   Communication Manager Messaging processes are stopped during RFU installation.

   If the RFU made modifications to the Messaging Administration Web page, you must close and reopen this page.

   Do not start the messaging software at this time.

Restarting the messaging application

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

Setting Communication Manager Messaging server parameters

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.

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

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 5: Testing Communication Manager Messaging

Adding test subscribers for messaging

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.

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

Prerequisites

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.

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

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