Administering Avaya Aura® Communication Manager Messaging

Release 7.0
Issue 1
November 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

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

License type(s)

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

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail

account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

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

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

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya and Avaya Aura® are registered trademarks of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 8
Purpose 8
Intended audience 8
Related resources 8
Documentation 8
Training 10
Viewing Avaya Mentor videos 11
Support 11
Warranty 12
Chapter 2: Communication Manager Messaging overview 13
Integration of Communication Manager Messaging with a Communication Manager server 13
Switch Integration Requirements 13
New features for Communication Manager Messaging release 7.0 14
Chapter 3: Architectural overview and feature descriptions 16
Messaging Concepts 16
What Is a Message? 16
What Is a Mailbox? 17
Telephone Access 18
System Architecture 19
Communication Manager server and Communication Manager Messaging Sever interoperability 19
Communication Manager Messaging Hardware 20
System features 20
Overview 20
Message Networking 21
Enhanced-List Application 21
Centralized Messaging Server 23
Voice messaging 24
Networking 25
Digital Networking 25
AMIS Analog Networking 28
Administration Tools and Utilities 28
INTUITY AUDIX Expert System overview 29
Chapter 4: Initial administration 31
Browser Requirements 31
Network configuration 31
Configuring the Communication Manager Messaging network 31
Enabling IPv6 33
Checking the Time Zone and NTP configurations 33

Messaging Basics ... 34
Login ... 34
Logging in to the Messaging System ... 35
Logging Out of the Messaging System ... 36
Administration passwords ... 36
Automated Attendant Administration ... 38
Assign a Station ... 38
Assign a Hunt Group ... 39
Night Service to Automated Attendant Administration ... 40
From an incoming trunk ... 40
From a Listed Directory Number (LDN) ... 40
Automated Attendant Substitute Strategies ... 41
Switch Recorded Announcement ... 41
Switch Multiple Coverage Paths ... 42
Support for * in outcalling dial strings ... 42
Chapter 5: Messaging administration ... 44
Administration ... 44
Overview ... 44
Administration Tasks ... 46
Administration and maintenance tasks checklist ... 49
Basic Messaging Administration ... 52
System administration ... 82
Subscriber Administration ... 91
Messaging system administration ... 107
Enhanced-List application administration ... 110
Digital networking administration ... 120
Remote user administration ... 137
Customizing announcements overview ... 147
Listing Announcement Sets ... 165
Account Code Billing administration ... 166
Automated Attendants and Bulletin Boards ... 170
Audits ... 198
Reports overview ... 201
Security ... 251
Fax Messaging ... 265
Email (Internet Messaging) ... 280
Chapter 6: Data managment ... 300
Overview ... 300
Backing Up System Files Now ... 303
Performing a Backup Now ... 304
Checking the backup status ... 305
Backing Up System Files (Scheduled) ... 306
Creating a new backup schedule ... 307

Change a backup schedule 308
Delete a backup schedule 308
Verifying a backup using the backup log 309
Restoring Backed-Up System Files 310
Performing a Restore (UNIX/Linux-based FTP Server) 310
Performing a Restore (Windows-based FTP Server) 312
Appendix A: Microsoft Outlook configuration 315
Appendix B: Centralized Messaging Server configuration 316
Configuring the Remote Server with translation data 316
Establish coverage path for Communication Manager Messaging 316
Setup routing to Centralized Messaging Server 317
Create tie trunk to the Centralized Messaging Server 317
Setup calling party number for call answer, otherwise hear ext 00000 319
Setup calling party number for login to messaging with # (extension not entered) 319
Setup routing of Message Waiting Indicator back to the remote server 320
Configuring the host server 320
Creating tie trunk to remote server 320
Appendix C: (Deprecated) Message Manager 323
Capabilities and Benefits 323
Requirements to Run (Deprecated) Message Manager 324
Messaging Enhancements 325
Planning Considerations 327
Addressing a Fax Message with (Deprecated) Message Manager 4.6 or Later 329
Creating a Fax Message with (Deprecated) Message Manager 4.6 or Later 330
PC Access through (Deprecated) Message Manager 330
(Deprecated) Message Manager Administration 331
Enabling Subscribers for (Deprecated) Message Manager 331
Enabling (Deprecated) Message Manager on an Individual Basis 332
Enabling (Deprecated) Message Manager by Defining a COS 333
Troubleshooting (Deprecated) Message Manager 333

Chapter 1: Introduction

Purpose

This book describes the procedures that are used for administering Communication Manager Messaging.

Intended audience

This document is intended for people who perform the product or solution system administration tasks.

Related resources

Documentation

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

Document number	Title	Description	Audience
Deployment			
	Deploying Avaya Aura® Communication Manager Messaging	Describes the deployment instructions for Communication Manager Messaging.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
	Deploying Avaya Aura® applications from Avaya Aura® System Manager	Describes the deployment instructions for Avaya Aura® using Solution Deployment Manager.	Solution Architects, Implementation Engineers, Sales

Table continues…

Document number	Title	Description	Audience
			Engineers, Support Personnel
Implementation			
	Implementing Avaya Aura® Communication Manager Messaging	This document describes the implementation process of Communication Manager Messaging.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Upgrade			
	Upgrading and Migrating Avaya Aura® applications to Release 7.0	Describes the upgrade for Avaya Aura® using Solution Deployment Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administration			
	Avaya Aura® Communication Manager Screen Reference, 03-602878	Describes the screens and fields of Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
	Administering Avaya Aura® Session Manager	Describes the administration instructions for Session Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel, Administrators
	Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Describes the network connectivity for Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel, Administrators

Finding documents on the Avaya Support website

About this task

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

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.

5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

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

Training

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

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

Table continues…

Course code	Course title
AVA00279WEN	Communication Manager - Configuring Basic Features
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00833WEN	Avaya Communication Manager - Call Permissions
AVA00834WEN	Avaya Communication Manager - System Features and Administration
5U00051E	Knowledge Access: Avaya Aura® Communication Manager Administration

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

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

Chapter 2: Communication Manager Messaging overview

Communication Manager Messaging is a voice, text, and fax messaging application.

Starting with Communication Manager release 5.2, Intuity Audix IA770 application is called Communication Manager Messaging.

You can install the Communication Manager Messaging software on any of the following servers:

- Dell™ PowerEdge™ R610
- Dell™ PowerEdge™ R620
- HP ProLiant DL360 G7
- HP ProLiant DL360p G8
- S8300D
- S8300E

Communication Manager Messaging utilizes the basic platform functionalities and cannot function without Communication Manager. Communication Manager Messaging application integrates with Communication Manager using SIP Trunk.

For details on installing and integrating Communication Manager with Communication Manager Messaging, please refer to *Deploying Avaya Aura® Communication Manager Messaging*. For specific information, visit http://support.avaya.com.

Integration of Communication Manager Messaging with a Communication Manager server

The following documentation provides information on the integration of Communication Manager Messaging with Communication Manager.

Switch Integration Requirements

Communication Manager Messaging uses information from the Communication Manager and Session Manager software to answer telephone calls, and also sends information back to the

Communication Manager and Session Manager software. Depending on the information received, the messaging software plays a greeting, provides an automated attendant, permits a subscriber to retrieve messages, or directs unanswered incoming telephone calls to the correct mailbox.

International Switch Tone Parameters

The messaging software supports many of the same country switch tone parameter sets established for the Communication Manager server.

The countries for which country-specific parameters are established are as follows:

- Brazil
- Canada
- China
- France
- Germany
- Italy
- Japan
- Mexico
- South Korea
- United Kingdom
- United States

New features for Communication Manager Messaging release 7.0

Communication Manager Messaging provides voice messaging for enterprises solutions. The Communication Manager Messaging software continues to use the basic platform functionalities of the Communication Manager software.

Communication Manager Messaging provides the following features:

- The subscriber telephone user interface (TUI) software
- Messaging software, which enables the messaging system to use lower level functions and includes the following capabilities:
  - Switch integration software

    This software allows call control messages (timestamps, calling party information, called party information, and message waiting indicator control) to pass between the messaging software and the Communication Manager software.
  - Virtual port software

    Communication Manager Messaging manages the voice message processing and emulates physical analog ports for sending and receiving voice messages.

- Event and alarm logging software

  This software logs alarms and sends them to the Communication Manager server Global Alarm Manager.

- Disk space management

  This software manages the portion of the Communication Manager server hard drive that is allocated to the messaging software.

- Digital networking
- Integration with standards based messaging systems

The Communication Manager Messaging 7.0 release has been enhanced to support software currency and interoperability with the Avaya Aura® 7.0 solution.

- The Linux OS is updated to Red Hat Enterprise Linux version 6.
- The Communication Manager Messaging application is integrated with the Appliance Virtualization Platform and Solution Deployment Manager.
- The Communication Manager Messaging application has been updated to support the Avaya SIP Reference Architecture and Security guidelines for encryption protocols.

Note that the following deprecated capabilities have been removed from the Communication Manager Messaging application with release 7.0:

- The Communication Manager Messaging application is no longer supported as an embedded application in Communication Manager. With Release 7.0, the application is installed as an instance of its own virtual machine.
- The H.323/Q.Sig integration is no longer supported, and has been removed. Customers should convert their Communication Manager Messaging application to a SIP integration prior to an upgrade to Release 7.0.
- The application migrations from Intuity Audix and Intuity Audix LX are no longer supported, and have been removed in prior Communication Manager Messaging 6.x releases. This capability to migrate within the backup and restore procedure is no longer supported in Communication Manager Messaging.

Chapter 3: Architectural overview and feature descriptions

Messaging Concepts

What Is a Message?

With Communication Manager Messaging, a message is not limited to voice components. A message may contain the following media type components:

- Voice
- Fax
- Text (created through Message Manager)
- File attachment (a software file, such as a spreadsheet or word processing file)

For example, a sales manager might want to inform the distributed sales force of a new compensation plan. The details of the compensation plan are in the form of a text message created in (deprecated) Message Manager or a standards based Email Client such as Microsoft Outlook. By using Communication Manager Messaging, the sales manager can send a message that consists of both voice and text components. The voice component of the message might be, "This message is going to all members of the Northeast Sales region. Congratulations on your excellent results last year. As of January 1, the compensation plan for new product sales will be changed. Please print the attached text message for detailed information." The text component of the message would then be used to specify the details.

When a message is sent, the messaging software adds descriptive information to the message consisting of the following information:

Header	The header consists of the time and date of delivery, the type of message, and a listing of all message components. The system automatically creates a header for each message sent. If a message is addressed to more than one recipient, the system creates a header for each recipient.
Message Body	The message body consists of the caller's spoken message or a voiced rendering of a text message, if using Text-to-Speech. In the case of a non deliverable message, the message body consists of a standard system message.

What Is a Mailbox?

A mailbox is a storage area on a computer disk for messages, personal greetings, and mailing lists. All Communication Manager Messaging subscribers automatically receive a mailbox when they are administered on the system. Mailboxes are divided into two sections, the incoming mailbox and the outgoing mailbox. Incoming messages are stored in an incoming folder and outgoing messages are stored in an outgoing folder. In addition, IMAP4 accessible server-side folders are available. These folders can be created, deleted, and renamed by IMAP4 clients. IMAP4 clients can be used to copy messages from the incoming folder to server-side folders and from the server-side folders to the incoming folder.

Each subscriber accesses his or her mailbox through a private password. After a subscriber logs in, the system voices the name of the subscriber (if recorded) and reports the number of new messages received (if any).

Incoming Mailbox

The incoming section of a mailbox receives messages from other subscribers, Communication Manager Messaging, and callers redirected to the mailbox because no one answered the telephone. The subscriber can save, delete, reply to, forward, and in other ways manipulate these messages.

A subscriber's incoming messages fall into three categories:

- New
- A message and header the subscriber has not yet listened to. The Message Waiting Indicator (MWI) on the subscriber's telephone turns on when a new message is present and turns off after the subscriber has listened to it.
- Unopened
- A message whose header has been listened to, but not the message itself. The MWI does not stay on for this type of message.
- Old
- A message the subscriber has listened to but has not deleted.

Outgoing Mailbox

The outgoing section of a mailbox stores the messages that a subscriber creates, sends, or forwards. In most cases, these messages remain in the outgoing section until they are delivered. Outgoing messages are of the following types (listed in the default order in which subscribers review outgoing messages). The system administrator can change this order, if desired.

- Files
- Messages that subscribers create and save in the outgoing section of a mailbox. Later they can access these messages to modify, address and send again, or delete.
- Undelivered
- Messages that have not yet been sent (for example, those scheduled for delivery at a future time or date). Subscribers can review, change, or cancel messages and their addresses at any time before delivery.
- Nondeliverable

- Messages that the system could not deliver. The system attempts to deliver a message up to 10 times (or the administered number of times) and then places the message in this category. Usually this indicates that the intended recipient's incoming mailbox is full, that the recipient's system cannot recognize or accept a message component, or that there were transmission problems.

  Messages defined as "nondeliverable" can be rescheduled for delivery with a new address, or altered to allow forwarding, if needed.
- Delivered
- Message headers that identify either messages delivered but not yet listened to or messages that contain components that could not be delivered. The latter type of message header is an Incomplete Deliveryheader. For example, if a message contains more than the allowable components (voice, text, and file attachments), the additional components are not delivered, and the message header indicates that a component was not delivered.
- Accessed
- Message headers that identify messages that have been listened to. A message is considered accessed even if only the header has been listened to.

Telephone Access

All message components can be manipulated from the telephone. The basic nature of the telephone interface remains the same, regardless of the component media type. Normally, messages are created, addressed, delivered, received, and replied to or forwarded. The following table shows how these actions are implemented when messages are accessed through the telephone.

Table 1: Message Manipulation from the Telephone Interface

Action	Component			
	Voice	**Text (created with Message Manager)**	**FAX**	**File Attachment**
Create?	Yes	No	Attach a fax when creating a message	No
Address?	Yes	N/A	N/A	N/A
Receive?	• Hear Message header • Hear voice	• Hear message header • Hear voiced rendering of message (requires Text-to-Speech)	• Hear message header • An indication of number of fax pages	• Hear message header • An indication of size (in Kb)
Print	N/A	Printed using TTF (text to fax).	• You can print to the default destination	Yes

Table continues…

Action	Component			
	Voice	**Text (created with Message Manager)**	**FAX**	**File Attachment**
			• Print to this fax machine • Print to a new destination	
Reply/Forward?	Yes You can include a voice/annotation.	Yes You can include a voice/annotation.	Yes You can include a voice/annotation.	Yes You can include a voice/annotation.

In summary, you can create voice messages with a telephone, but you cannot create text messages and file attachments with a telephone. When retrieving messages, you can listen to voice and text messages. You can print messages to a fax machine using the TUI. You can print messages to a printer using (deprecated) Message Manger or from a standards based email client like Microsoft Outlook.

System Architecture

Communication Manager server and Communication Manager Messaging Sever interoperability

Communication Manager and Communication Manager Messaging are interoperable and are integrated using SIP protocol.

Communication Manager server

The Communication Manager server comes loaded with the following resources:

- Red Hat Enterprise Linux Version 6 operating system
- Web server software
- SIP protocol
- Communication Manager software, which serves as the primary voice/data communications application

The Communication Manager server serves as a full-featured integrated data and phone communication system. The Communication Manager server has its own virtual machine.

Disk Partitioning

The disk partitioning scheme has three partitions (two active and one duplicate).

The layout of active partitions used by the Communication Manager server products is defined as follows:

- /msg/software: for messaging software, database, and add-on applications. Symbolic links, references to mount points, and so on are modified as needed to preserve the existing directory structure. The size of this partition is at least as large as the sum of the replaced three partitions on the latest Communication Manager server product.
- /msg/media1: for the message bodies. The size of this partition is at least as large as the existing partition on the latest Communication Manager server product.

Communication Manager:

- Is used to create stations, coverage path, trunk groups
- Is on a different virtual machine than Communication Manager Messaging

Communication Manager Messaging Hardware

Media Modules

No media modules required for Communication Manager Messaging.

Ports

Communication Manager servers have a serial port. This serial port can be used for a direct connection to a laptop or PC. The port is called **Service** on the S8400 Server.

Terminals

You can administer the system through the use of a SSH session and one of the following terminal emulations:

- vt100
- xterm-r6

This section discusses the hardware and software components that make up Communication Manager Messaging.

System features

Overview

The customer can select from various optional software and hardware components to build a Communication Manager Messaging system. Some components are optional units, usually made up of hardware and software, which can be added to the base system. The primary software applications reside on the same platform. This allows users to share resources, such as hard disk space, and database information.

Messaging system features related to administration, maintenance, and reliability are discussed in Administration on page 44.

Message Networking

Message Networking is a server-based solution that links individual voice or multimedia messaging systems from multiple vendors into a company-wide messaging network. The Message Networking system supports transport and protocol conversion of the following networking protocols:

- Communication Manager Messaging Digital
- Octel Analog
- Aria Digital
- Serenade Digital
- VPIM v2 Digital

The system automatically transcodes message formats among all supported networking protocols. As a result, if you have the digital networking features of the messaging system, Message Networking allows you to network your subscribers with subscribers on other Avaya and non-Avaya systems. For example, Message Networking allows subscribers to send messages between the following messaging systems:

- Communication Manager Messaging
- DEFINTIY AUDIX R3.2
- INTUITY AUDIX release 3.3 and later
- IA 770 INTUITY AUDIX
- IP600 R9.2.1
- Aria Version 1.0 and later
- Serenade Version 2.0 and later
- Non-Avaya systems that support VPIM v2
- Modular Messaging
- Aura Messaging
- Avaya Call Pilot

See the Message Networking-related documentation for more detailed information.

Enhanced-List Application

The Enhanced-List Application (ELA) greatly expands the capability to deliver messages to large numbers of recipients. A single enhanced-list can contain 1500 addresses. The system administrator can create up to 100 enhanced-lists.

ELA features

Enhanced-List Application (ELA) provides the following features:

- Up to 1500 recipients can be contained in an enhanced-list.
- Up to 100 enhanced-lists can be created on an Communication Manager Messaging system.
- Changes in an enhanced list propagate to all lists that refer to the changed list.
- Access to enhanced-lists is possible from anywhere within the Messaging network (standard Communication Manager Messaging mailing lists are accessible only to those subscribers with mailboxes on the same machine as the lists).
- Messages can be delivered to local, remote, and email subscribers.
- Messages can be delivered across domains from a standards based email client to Communication Manager Messaging. This kind of delivery enables email subscribers to access the enhanced-lists.

With ELA, you can:

- Distribute messages to a targeted audience.
- Create a list of people to whom you send messages frequently. Then send all these people the same message by entering one enhanced-list address.
- Centralize messages in one Communication Manager Messaging mailbox.
- Select one office as your primary location. Then, create an enhanced-list at each secondary location that has as its only member the number of your primary office location. When a mailbox at a secondary location receives a message, ELA puts it into the mailbox for the primary office.
- Forward messages to support staff automatically.
- If you frequently forward incoming messages, create an enhanced-list mailbox that automatically forwards messages to other subscribers. These subscribers can review the messages and then respond to them as they normally would.
- Nest (or embed) enhanced-lists.
- A list with 1500 addresses can be a list contained within another list. Thus, a subscriber can record a message, address it to the parent enhanced-list, and send it to nearly 150,000 people just as easily as if the message were being sent to only one person seated at the next desk.

All subscribers administered in Communication Manager Messaging (including email and remote subscribers) can send messages to the recipients in enhanced-lists. Or, you can administer your system to allow only selected subscribers in your Communication Manager Messaging network access to the enhanced-lists.

ELA Security Considerations

When you are securing a system that allows access from another domain, you must consider both internal and external security.

External Security

External security involves administration to prevent access from an unauthorized source. These sources can include a subscriber who is administered to use email. Users might send "spam" to an enhanced-list. Spam are harassing messages that not only do not serve your business needs and impose unnecessary traffic on your system.

ELA mailboxes are no more vulnerable to unauthorized use than are any other voice mailboxes. However, the impact on system performance can be many times greater.

To prevent unauthorized access to an ELA mailbox from an external source such as email users, you can place those subscribers in a community with sending restrictions.

Internal Security

Internal security focuses on preventing or recovering from damage if a breach occurs, for example, if a virus is transmitted in a message component such as an attached software file.

Communication Manager Messaging allows for the transmission of two message components, text (originating from Message Manager or email) and binary file attachments (software files, such as a spreadsheet or word-processing file). With these components come related security considerations, namely, the inadvertent delivery of a computer virus that could be embedded in a file attachment. This problem can occur in any system that supports the delivery of software files. While the Messaging server cannot be infected with viruses embedded in these software files, client machines can become infected when a user launches the application associated with the software file.

Note:

ELA does not perform any virus detection. The customer needs to evaluate the security risks of file attachments carefully and make provisions for virus detection software on PCs running Message Manager or an email application supported by Communication Manager Messaging.

At a minimum, advise your users to detach (that is, not launch) file attachments and scan them for viruses before use.

Centralized Messaging Server

You can configure a server with Communication Manager Messaging application installed on it as a Centralized Messaging Server (CMS). As part of the configuration for Centralized Messaging Server you need to define SIP trunks between the host Communication Manager and the remote Communication Manager.

The configuration supports messaging mailboxes on one Communication Manager server (Centralized Messaging Server) and provides voice mail coverage for phones (stations) on a second Communication Manager server (remote server).

To set up the Centralized Messaging Server, you need to add the configuration changes in the form of switch translations by using the System Access Terminal (SAT) on both Communication Manager servers. Centralized Messaging Server supports features such as, Calling Party Number (CPN) and Message Waiting Indicator (MWI).

Voice messaging

Subscribers can record a spoken message, address it, and then send it to other voice messaging subscribers. These users can receive the message on their local machine or on networked messaging systems.

Subscribers instruct the voice messaging system by pressing the keys on their touchtone telephones in response to detailed voice prompts from the system.

Voice Messaging Features

Voice Messaging provides the customer with four primary features:

- Voice Messaging
- Call Answer
- Automated Attendant
- Bulletin Board

Voice Messaging

Voice Messaging is similar to an electronic mail system in that messages can be sent to others without the sender's needing to call the recipient directly. The message is then stored in the recipient's voice mailbox. Recipients can access stored messages at their convenience.

Voice Messaging enables the subscriber to:

- Send messages to other messaging subscribers.
- Listen to messages received from other messaging subscribers.
- Forward messages received with comments attached.
- Reply to messages received from other messaging subscribers.
- Create mailing lists that can contain up to 250 recipients.

In addition to these basic capabilities, the outcalling feature of Voice Messaging also enables the subscriber to:

- Automatically place a call from messaging to the subscriber when there are new messages waiting.
- Specify the telephone number to be called by messaging when new messages are waiting. This telephone number can be for an office, home, or cellular telephone, or for a pager.

Call Answer

Call Answer enables subscribers to:

- Have the messaging system answer incoming telephone calls.
- Create personal greetings that voice messaging uses to answer incoming calls.

In addition to these basic capabilities, Call Answer also enables the subscriber to:

- Customize a set of standard greetings.
- Record up to nine different personal greetings through the Multiple Personal Greeting feature.

- Play a single greeting for all calls or assign various personal greetings to be played in response to different types of calls, for example, internal and external, busy and no answer, and/or out-of-hours.

Automated Attendant

An automated attendant is an interactive telephone answering system. It answers incoming calls with a prerecorded announcement and routes the calls based on the caller's response to menus and prompts.

The system administrator sets up an automated attendant so that callers hear a menu of options. Callers then press the button on their telephone keypad that corresponds to the menu option that they want, and the automated attendant executes the selected option. Those calling from rotary telephones are typically told that they can hold or call another number to speak with a live attendant.

An automated attendant menu system, or menu tree, can be designed to contain subordinate layers of menus or bulletin boards. These submenus, or nested menus, play additional options that can include a choice that leads to another nested menu.

The voiced menu options that callers hear are actually personal greetings that the subscriber records for the automated attendant's extension. The text of the message can be changed just as easily as any personal greeting can. The Multiple Personal Greetings feature can be used to provide different menus and options for different types of callers.

Bulletin Board

A bulletin board is an electronic message system that callers can access to hear messages. Callers dial the bulletin board telephone number, and the system answers and presents a recorded message. The major difference between a bulletin board and an automated attendant is that a bulletin board does not have an option to route to a live attendant. For more information, see Automated Attendants and Bulletin Boards on page 170.

Networking

Networking provides the capability to transfer message components among customers located on different systems. Depending on the type of networking and the specific types of systems involved, these components can include voice messages, text messages, and attachments.

This section provides information about networking a new messaging system, including network capacities, connectivity, channel support, features, and operation.

Digital Networking

Digital Networking is an optional feature that provides customers with the ability to exchange messages with customers on other messaging systems by using TCP/IP. The remote system can be located either at the same location as the local messaging system or at a different location.

This topic provides information on the following:

- How Digital Networking works on page 26

- Capacities on page 26
- Features on page 26

When you are ready to administer the Digital Networking feature, see Digital Networking Administration on page 120.

How Digital Networking Works

The Digital Networking feature package supports the TCP/IP protocol over an Ethernet connection to local and wide area TCP/IP networks. Data connections serve both local and remote networking, depending on the customer's system configuration. Digitally transmitted messages are communicated quickly and with excellent sound quality.

Digital networking provides subscribers with the ability to exchange voice messages, text messages, and attached files from networked sources, including:

- Messages from subscribers on other Avaya messaging systems
- Message Manager text components
- Email messages with arbitrary attachments

Audix Digital Networking

The Digital Networking feature uses the proprietary Avaya digital protocol to exchange messages, subscriber profiles, and message status information with other machines. The digital protocol uses a digital file format, similar to a data file transfer between two computer systems, to transmit the information.

LDAP/SMTP networking

Remote Subscriber information is transmitted using the standards-based LDAP protocol, while messages are transmitted using the standards-based SMTP protocol.

Digitial Networking Capacities

Digital networking supports a maximum of 500 remote machines. The system supports a maximum of 60,000 to 70,000 total administered and nonadministered remote subscribers. The total number of networked systems and remote subscribers depends on the amount of available storage.

For the Audix Digital Networking, the messaging system provides a maximum capacity of 8 channels of digital networking.

Digital Networking Features

Subscribers who want to send Digital Networking messages to recipients on administered remote systems can:

- Address their messages by name. This feature applies only to administered remote recipients. "Administered" refers to remote subscribers who are entered in the database of the local messaging system either manually or through an automatic update.
- Include the names and telephone numbers of remote recipients in their personal mailing lists. Nonadministered remote recipients are included only by telephone number.

- Hear the spoken name of the person to whom they are addressing mail or are looking up in the directory. If the administrator has not recorded these names or if the names have not been received in a remote update, subscribers hear only the remote mailbox ID.
- Use the names and number directory (* * N) to look up telephone numbers by name.
- Assign aliases to any remote recipients on systems administered for Digital Networking. Administered remote recipients can be included by name or telephone number. Nonadministered remote recipients can be included by telephone number only.
- Use automatic addressing to reply to incoming messages.

Digital networking enhances the messaging system in these ways:

- Customers with business offices in more than one location, whether in the same building or in different cities, can exchange messages with all locations.
- Customers who exceed the capacity of one messaging system at a location can network multiple machines together to enable subscribers to exchange messages as if they were on the same machine.
- The following message-exchange features are available for messages exchanged between remote subscribers:
  - The ability to address a message by entering a subscriber's name. This is called name addressing.
  - The ability to play a recorded name, if a name is recorded for the remote subscriber, when a subscriber addresses a message to the remote subscriber or when the subscriber receives a message from the remote subscriber.
  - The ability to forward messages to one subscriber or a group of subscribers, respond to messages, and create group mailing lists.

    Note:

    Mailing lists cannot be shared across the network.
- The quality of the voice message received is the same as when it was recorded, no matter how many times the message is forwarded.
- Local and remote subscriber databases are updated automatically with the remote update feature.
- Customers with businesses that operate in different time zones can send or receive messages any time of day or night.
- All that a digital networking subscriber needs to know to exchange messages with remote subscribers is the machine prefix and remote subscriber extension or, if using the name addressing feature, only the subscriber's name.

TCP/IP networking for add-on applications

Communication Manager Messaging 6.3 and 7.0 support TCP/IP for Audix digital networking. TCP/IP networking uses the Ethernet connection of the Communication Manager server. The Ethernet connection enables the messaging software to connect to a customer's LAN.

TCP/IP network access is automatically available with the messaging software through the TCP/IP connections of the Communication Manager server, and no specific TCP/IP administration for the messaging software is required.

Internet Messaging is an optional add on application that operates with messaging. For more information see Internet Messaging on page 280.

AMIS Analog Networking

Note:

Communication Manager Messaging does not support administration of AMIS networked connections.

Administration Tools and Utilities

Communication Manager Messaging provides several tools and utilities that are available to enhance the system administration environment including:

INTUITY AUDIX Expert System

Since 1987, AT&T's, and now Avaya's, Services organization has used artificial intelligence technology in the form of expert system tools, in conjunction with its human technicians, to provide its customers with first-rate maintenance support. Your messaging software is supported by the INTUITY Audix Expert System, which is a computer system that facilitates solving problems in a given field or application by drawing inference from a knowledge base developed from real-life experiences. The Expert System works in the background by collecting data from a remote location. It is not an interactive tool.

For more information on how this Expert system works, see INTUITY AUDIX Expert System on page 29.

Backup and Restore

The Communication Manager server backs up messaging data to a remote SFTP/FTP server. In the event of a system failure, the information stored on this remote server is used to restore the system back to an operational state.

There are two types of backups, Scheduled Backup on page 28 and Backup Now on page 28.

Note:

A Backup Now cannot run during a Scheduled Backup. A scheduled backup cannot run during a Backup Now.

Scheduled Backup

The messaging system can regularly and automatically back up information critical to its operation. This kind of backup is called a Scheduled Backup. The administrator defines exactly when the backup occurs and what data is backed up by using the Communication Manager server backup

administration web pages. In the event of a system failure, some voice messages could be lost from the time of the last backup.

Backup Now

In addition to the information saved during the scheduled backups, an administrator can manually copy information from the messaging system to the backup server for security and recovery purposes at any time. This is called a Backup Now.

Note:

Establish a regular, rigorous backup schedule based on the quality of service you plan to provide to your subscribers.

Avaya recommends performing a Backup Now at all of the following times:

- After making major system changes
- After entering new subscribers
- When experiencing system problems to avoid losing information entered since the last unattended backup

Related Backup and Restore Information

For details on using these capabilities, see the online Help system available from the **Server (Maintenance)** Web page or the maintenance documentation on the Communication Manager documentation that can be downloaded from Avaya Support Site.

INTUITY AUDIX Expert System overview

The INTUITY Audix Expert System performs remote diagnostics in response to alarms reported by the customer's products to the Technical Service Center's alarm-receiving system. In addition, the tool collects data from the product to assess many internal conditions that could be indicative of a potential problem to the customer. For example, the tool can assess these types of potential problems:

- System reboots, to check on resource utilization
- Available ports and disk space
- Identify failure signatures that might not have yet created alarms

Trouble tickets are annotated with results from the expert sessions, which can include ticket closure for the alarm problem, referral to a human technician for further analysis, referral to customers as a facility (non-AVAYA product) problem, and/or a technician dispatch recommendation with needed parts identified.

In addition to standard maintenance documentation, expert system diagnostics are based on the most recent field and development knowledge and the product's internal data records. Extensive databases provide details that explain why a particular recommendation was made. These recommendations, called Product Performance Recommendations (PPRs), can be accessed by a field technician for on-site repairs or by a TSC technician when a call to the customer is required. Regular reviews of the data by Services and Avaya Labs provide improved diagnostic effectiveness of the expert system tests and recommendations. Technicians also have online access to PPR

descriptions so that any changes in diagnostics in the expert systems are immediately available to technicians.

For example, if a messaging system starts showing signs of a limited amount of hard drive space, an alarm is reported to the alarm-receiving system. A trouble ticket is created and assigned to the Expert System, which then connects to the product and analyzes this alarm and can execute the appropriate commands to clear the condition. Trouble tickets are annotated with results from the expert sessions, and the ticket then can be closed. If the condition requires human intervention, the Expert System's monitoring staff then notifies the customer recommending that the customer increases the hard drive storage.

Chapter 4: Initial administration

Browser Requirements

Communication Manager Messaging supports the following browsers:

- Internet Explorer 10.0 and later
- Mozilla Firefox 39.0 and later

Network configuration

Use the Network Configuration page to configure the IP-related settings for the virtual machine.

Note:

Some changes made on the Network Configuration page can affect the settings on other pages under the **Server Configuration** page. Ensure that all the pages under **Server Configuration** have the appropriate configuration information.

Using the Network Configuration page, you can configure or view the settings of the hostname, alias host name, DNS domain name, DNS search list, DNS IP addresses, server ID, and default gateway.

If the configuration setting for a field is blank, you can configure that setting on the Network Configuration page.

The virtual machine uses virtual NICs on virtual switches internal to the hypervisor.

The system uses eth0 in most cases.

Configuring the Communication Manager Messaging network

About this task

Before using Communication Manager Messaging, you must complete network configuration.

Procedure

1. Log on to Communication Manager Messaging System Management Interface, with the Customer Privileged Administrator account user name and password that you created during deployment.

2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Network Configuration**.

   The system displays the Network Configuration page.
4. On the Network Configuration page, type appropriate values for network configuration.

   If you do not enable IPv6, you cannot configure the IPv6 fields.
5. Click **Change** to save the network configuration.

Network Configuration field descriptions

Name	Description
Host Name	The host name of the virtual machine. You can align the host name with the DNS name of the virtual machine. Do not type underscore (_) in the **Host Name** field.
DNS Domain	The domain name server (DNS) domain of the virtual machine.
Search Domain List	The DNS domain name of the search list. If there are more than one search list names, separate each name with commas.
Primary DNS	The primary DNS IP address.
Secondary DNS	The secondary DNS IP address. This field is optional.
Tertiary DNS	The tertiary DNS IP address. This field is optional.
Server ID	The unique server ID, which is a number between 1 and 256. On a duplicated virtual machine or survivable virtual machine, the number cannot be 1.
IPv6 is currently	Specifies the status of IPv6. The options are: enabled and disabled.
Default Gateway IPv4	The default gateway IP address.
Default Gateway IPv6	The IPv6-compliant IP address of the default gateway.
IP Configuration	The set of parameters to configure an Ethernet port, such as, eth0, eth1, or eth2. The parameters are: • **IPv4 Address** • **Mask** • **IPv6 Address** • **Prefix** • **Alias IP Address: IPv4 Address** (for duplicated virtual machines only) • **Alias IP Address: IPv6 Address** (for duplicated virtual machines only) **Note:** You can configure as many Ethernet ports as available on the NICs of your virtual machine.

Table continues…

Name	Description
Functional Assignment	Based on the system configuration, the system displays the following options. • Corporate LAN/Processor Ethernet/Control Network • Corporate LAN/Control Network • Duplication Link • Out-of-Band Management **Note:** When you select the Out-of-Band Management option, the system displays the **Restrict Management traffic to Out-Of-Band interface is currently** field.
Restrict Management traffic to Out-Of-Band interface is currently	The possible values are: • enabled: restricts the management traffic to Out-Of-Band interface. • disabled: allows the management traffic to Out-Of-Band interface. By default the value of this field is set to disabled.

Enabling IPv6

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Server Configuration** > **Network Configuration**.

   The system displays the Network Configuration page.
4. From the **IPv6 is currently** drop-down list, select enabled.
5. Click **Change** to enable the IPv6 fields.

Checking the Time Zone and NTP configurations

About this task

The messaging system uses the Linux system clock to perform certain time-dependent tasks, such as placing a time stamp on voice messages and doing the nightly backup of critical system data.

Procedure

On the Server (Maintenance) Server Configuration web page, do the following:

a. Check the Time Zone Configuration

   After the time zone is changed, you must reboot the server to ensure that all processes pick up the new time settings.

b. Verify the NTP Configuration.

Messaging Basics

Login

You can create a custom login account and associate it to a Communication Manager profile based on the web pages the user must access. The Communication Manager Messaging application uses the user-based profiles created by Communication Manager. User profiles enable you to allow a user to access only a specific set of administration web pages.

For example, the privileged administrator account uses the Communication Manager user profile 18. This profile provides access equivalent to a customer super-user login.

The unprivileged administrator account uses the Communication Manager user profile 19 which is equivalent to a customer non super-user login.

You can add logins from the **Server (Maintenance)** > **Web page** > **Security** > **Administrator Accounts**.

Messaging login types

Login	Definition	Allows you to access:
Privileged Administrator	System administrator	• All Communication Manager Messaging Web-based administration pages
Unprivileged Administrator	Voice messaging administrator	• Most Communication Manager Messaging Web-based administration pages
craft	Services technician	• All Communication Manager Messaging Web-based administration pages • All Communication Manager server Web-based administration screens

Table continues…

Communication Manager Messaging access only	A User with only Communication Manager Messaging access only	All messaging web pages
Custom	Assign a Communication Manager profile to this login	Depending on the profile associated to this login, the user is able to view associated web pages

After an upgrade to Communication Manager Messaging you should create a login and assign the existing profile to the new login. Alternatively you can use the same login account and provide more permissions to the existing profile.

Your service technician installs your system with default administrator passwords. You need to immediately change these administrator passwords after the installation is complete. After familiarizing yourself with the basic operations of the messaging system detailed in the next few sections, set a new administrator password. For more information, see Changing administration password on page 37.

Note:

A user can do messaging administration from custom created logins, but when a custom login is created, assign **Voice** as the access profile in the **Additional Groups** text box.

Go to the Server Administration page and click **Security** > **Administrator accounts** to add a custom login.

In addition, you should review the Security page and Login Account Policy page for the following:

- Password Complexity Requirements
- Login Inactivity Timeout
- Credential Expiration Parameters
- Failed Login Response

Logging in to the Messaging System

Procedure

1. Open a compatible Internet browser on your computer desktop.

   Currently Internet Explorer 10.0 and later and Mozilla Firefox 39.0 and later are supported.

   The system displays your Internet Home page.

2. In the Address (or Location) field of your browser, type the IP address or hostname of the Communication Manager Messaging server and press `Enter`.

   If your browser does not have a valid security certificate, the system displays a warning with instructions to load the security certificate.

3. Follow the instructions that the system displays and load the security certificate.

   The system displays the Avaya Security Notice screen.

4. Click **Continue**.

   The system displays the Logon screen.

5. In the **Logon ID** field, type your login ID, and press `Enter` or click **Logon**.

   The system displays the Password field or the Access Security Gateway (ASG) challenge.

6. Type your password (initially you get this from your installer) or the correct ASG response and press `Enter` or click **Logon**.

   The system displays the Messages screen which shows information about Last login, Last failed login, and failed login attempts since the last successful login.

7. Click **Continue**.

   The system displays the Communication Manager Messaging System Management Interface page.

8. On the **Administration** menu, click **Messaging**.

   The system displays the Messaging Administration page.

   You can use the options displayed in the **Messaging Administration** section to administer Communication Manager Messaging

Logging Out of the Messaging System

About this task

To log out of the Messaging System:

Procedure

On the Messaging Administration page, click **Log Off**.

Administration passwords

You must immediately change the password for your login account after your system is installed. Establish a regular schedule for changing the password, for example, at least monthly. You must inform any other messaging administrators or system administrators of the change in passwords.

Both system administrators and messaging administrators can change passwords. Messaging administrators who log in with a non-privileged administrator account can only change the password for that account. System administrators who log in with a privileged administrator account can change a password for the privileged and non-privileged administrator logins.

Note:

To change administrator passwords, you must log in to the Communication Manager Messaging server web interface using the dadmin login and password. If dadmin does not exist, you must create a dadmin account that is part of the susers group.

Additionally, you can administer several parameters of the password aging feature that will enhance the level of security that the system maintains.

This section provides the procedures for changing passwords by setting password aging.

Note:

For information about administering subscriber default passwords and password aging, see Reassigning Subscriber Default Passwords on page 104.

Guidelines for Administrator Passwords

To minimize the risk of unauthorized people using the messaging system, follow these guidelines for system administrator passwords.

- Establish a new password as soon as the messaging system is installed.
- Use from 6 to 11 alphanumeric characters. The password must include at least one numeric character and two alphabetic characters.
- Never use obvious passwords, such as a telephone extension, room number, employee identification number, social security number, or easily guessed numeric or letter combinations.
- Do not post, share, print, or write down passwords.
- Do not put the password on a programmable function key.
- Change the password at least once per month. You can administer your system to age the password and notify you that a new password is required.

Changing administration password

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the **Security** section, click **Administrator Accounts**.

   The system displays the Administrator Accounts page.
4. In the **Select Action** section, click **Change Login**.
5. In the **Select Login** field next to the **Change Login** field, click the login whose password you want to change.
6. Click **Submit**.

   The system displays the Administrator Accounts – Change Login page.
7. Select the **Select type of authentication** check box.
8. Click **Password**.
9. In the **Enter password or key** field, type the new password.
10. In the **Reenter password or key** field, type the new password again.
11. In the **Force password/key change on next login** field, click **Yes**.

12. Click **Submit**.

Setting password aging

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the **Security** section, click **Login Account Policy**.
4. In the Credential Expiration Parameters section, provide appropriate values in the following fields:
   - The maximum number of days a password may be used (PASS_MAX_DAYS)
   - The minimum number of days allowed between password changes (PASS_MIN_DAYS)
   - The number of days a warning is given before a password expires (PASS_WARN_AGE)
   - The number of days after a password expires to lock the account (INACTIVE; 0 = immediate, 99999 = never)
5. Click **Submit**.

Automated Attendant Administration

Automated attendant is a messaging feature that provides the caller with a menu of options. The caller then can request a department or extension by pressing a touchtone key.

For each attendant, assign a messaging hunt group for the extension of the attendant.

Assign a Station

About this task

You can assign a station on the switch for each main attendant. The station requires a physical port on the switch. A physical voice terminal is not required. However, if a voice terminal is not attached to the port, the switch generates a minor alarm.

Use the following procedure to assign a station for a main attendant:

Procedure

1. Assign a station for the type of available port.

   See *Administering Avaya Aura® Communication Manager* for information on assigning a station.

2. Do one of the following:
   - If you are using the automated attendant as an incoming destination for a trunk group, assign the station extension as the incoming destination for the incoming call trunk groups that will be served by the automated attendant.
   - If you are not using the automated attendant as an incoming destination for a trunk group, do the following:
     a. Confirm that the **Auth Code field** is set to `n`.
     b. Continue with step 3.
3. From the attendant console or administrative voice terminal, activate **Call Forwarding All Calls** for the automated attendant extension.

   Make the destination the messaging hunt group extension.

Assign a Hunt Group

About this task

Assign a new hunt group for the automated attendant if there is not a physical port available on the switch for a station. The hunt group forwards calls to the messaging hunt group. Use the following settings to assign a hunt group for the automated attendant.

To assign a hunt group:

Procedure

1. Set **Group Name** to a name that contains the group extension.

   Use the group extension as all or part of the group name.
2. Set **Group Extension** to the automated attendant extension.
3. Set **Group Type** to **ucd**.
4. Leave the **Coverage Path** field blank.

   All calls are forwarded to the messaging hunt group extension.
5. Set the other fields according to the customer requirements.
6. Set **Queue?** to **y**.
7. Assign the numbers of all trunks to the hunt group.
8. Click **Save**.
9. Assign the automated attendant group extension as the incoming destination for incoming call trunk groups served by the automated attendant.
10. If you are not using the automated attendant as an incoming destination for a trunk group, skip this step and continue with Step 11.

    Set **Auth Code** to **n**.

11. At the attendant console, activate Call Forwarding All Calls for the automated attendant.

    Set the destination as the messaging hunt group extension.

Night Service to Automated Attendant Administration

You can set up night service to an automated attendant from an incoming trunk or from a Listed Directory Number (LDN).

From an incoming trunk

About this task

Use the following procedure to set up night service to an automated attendant from an incoming trunk:

Procedure

1. At the SAT command line prompt, type `change trunk-group n`, where *n* is the trunk group number.
2. Assign the night automated attendant extension or hunt group number to the **Night Service** field on the Trunk Group screen.

   The night automated attendant receives all incoming calls when you activate night service.
3. Activate Call Forwarding All Calls for the night automated attendant extension or hunt group number.

   Set the destination as the messaging hunt group extension.

Result

While the console is in day service mode, calls are routed as usual according to the incoming destination on the Trunk Group screen. When the console is placed in night service mode, calls are routed according to the night automated attendant destination identified in the **Night Service** field.

From a Listed Directory Number (LDN)

Procedure

1. At the SAT command prompt, type `change listed-directory-numbers`.
2. Assign one or more unique extensions on the Listed Directory Numbers (LDN) screen.

These extensions cannot exist elsewhere in the switch. For example, assign 5000 as the LDN.

3. For each extension assigned in Step 2, assign a name that includes the night automated attendant extension or hunt group number as part of the name.

   For example, if the night AA number or hunt group number is 5001, use the name night5001.

4. At the SAT command prompt, type `change hunt-group n`, where *n* is the hunt group number.

5. Assign the messaging hunt group extension in the Night Destination field.

   From the examples above, this number would be 5001.

Result

When you place the attendant console in day service mode, the LDN acts as usual. When you place the attendant console in night service mode, the system sends calls to the messaging hunt group extension. The messaging software answers calls by using the automated attendant that corresponds to the number in the **LDN Name** field.

Automated Attendant Substitute Strategies

A substitute for an automated attendant is needed so that calls do not go unanswered when the messaging software is busy or unavailable. Administer each messaging system individually. Consult the appropriate switch documents for details and interactions with other features.

For the automated attendant, you assigned either a station or a hunt group. If you assigned a station, you cannot use a substitute. If you used a hunt group, and messaging is unavailable, use the attendant console to change the destination of Call Forwarding from the messaging system to a live attendantfor example, forward calls to LDN. When messaging becomes available, activate forwarding to the messaging extension. Another option is to change the incoming destination to a recorded announcement while the automated attendant is out of service. See Switch Recorded Announcement on page 41 below for more information.

Switch Recorded Announcement

About this task

The following procedure is used to provide a recorded announcement at the switch for anyone who accesses messaging, either through a direct call or through call redirection. The announcement is heard when all the messaging system voice ports are busy and calls start to enter the messaging system queue.

Note:

Announcements must be downloaded from a web server and stored in the Announcements directory.

- At the administration terminal, enter **change announcements**.
- On a vacant line, from 1 to 64, set **Ext** to the extension number. The number must agree with the dial plan.
- Set **Type** to **Integrated**.

Procedure

1. Set **COR** from 0 to 63.
2. Set Name.

   (You can use up to 15 characters to describe the announcement message.)
3. Set **Queue** to **y**.
4. Enter **n** in the **Protect** field.
5. If you set the **Typ** e field to **integrated**, enter **16**, **32**, or **64** in the **Rate** field to specify the recording speed when recording announcements.
6. Press Enter to save the information and return to the **enter command** prompt.
7. Enter **change hunt-group 59**.
8. Enter the extension of the announcement system in the **First Ann. Extension** field.
9. Enter **5** in the **First Announcement Delay (sec)** field.
10. Press Enter to save the information and return to the **enter command** prompt.
11. Dial the announcement's extension number from the console or from a voice terminal with a console COS.

Switch Multiple Coverage Paths

Multiple coverage paths provide greater flexibility for call-answer treatment. On the Coverage Path screen, specify a second path in the **Next Path Number** field. You can link the second path to other paths. These paths are displayed in the **Linkage** field. For more details, see Administrator's Guide for Communication Manager, 03-300509.

Support for * in outcalling dial strings

About this task

The outcalling feature alerts subscribers to the presence of new messages by placing calls to them.

Communication Manager Messaging supports * in the outcalling dial string when used in Communication Manager. Communication Manager Messaging treats the * as a pause in the outcalling string. For example, if you want to call a company and then an internal number, you can separate the numbers with a *. For example, to reach a company number 230001 and then the internal number 5823, you can dial 230001*5823.

Procedure

1. While configuring Communication Manager, add * as a feature access code.
2. Change appropriate fields on the Change Feature Access Code page.

   For example, *9.
3. On the Messaging Administration Web page, click **Outcalling Options**.
4. Set the **Outcalling Active** field to `Yes`.
5. To test the * functionality:
   a. Log in to the mailbox of a user using **Telephone User Interface**.
   b. Press *9.

      You are in the outcalling menu.
   c. Set up the outcalling to be another number.
   d. Turn on outcalling for all new messages.
   e. Send a message to the subscriber.
   f. Verify that ***** in outcalling acts as a number.

Chapter 5: Messaging administration

Administration

Overview

This overview contains a variety of topics that relate to initial and ongoing administration of Communication Manager Messaging.

Administrative Interfaces

The system provides two interfaces for accessing and administering messaging features. These interfaces are:

- Telephone User Interface
- The Communication Manager Messaging server browser interface

The browser interface can be used from any location with access to the internal LAN or the Internet. Some of the initial administration is a must before administering the Communication Manager Messaging server. Therefore, the system administrator might use the Communication Manager server browser interface to backup or restore messaging data, check system status, and check alarms.

From the Communication Manager server browser interface, the administrator also accesses the web administration pages, from which a large number of tasks can be performed, including administering Internet Messaging, checking channel status, and accessing logs. Through the messaging web pages, the system administrator can:

- View information, enter information, access menus, or select available system options.
- Access online system Help and field Help for data entry fields in the window.

Note:

Services technicians can bypass the LAN and access the Administrative Web Interface by using a direct connection from their laptop to the Communication Manager server services port. For details on how to access the Communication Manager server, see Administering Communication Manager servers to work with Communication Manager Messaging .

Administration from the Telephone Interface

The system administrator performs some administrative tasks by using the telephone, including recording:

- Subscribers' names. This task is optional. Customers can record their own names.

- Networked machine names. For information on networking, see Digital Networking Administration on page 120.
- Automated attendant menus and options.

The voiced menu options that callers hear are actually personal greetings that the customer records for the Automated Attendant's extension. The Multiple Personal Greetings feature can also be used to provide different menus and options for different types of callers. For an overview of the Automated Attendant features, see Automated Attendants and Bulletin Boards on page 170.

- Bulletin Board announcements.

As with Automated Attendants, the system administrator records Bulletin Board messages. For more information and procedures, see Automated Attendants and Bulletin Boards: What Is a Bulletin Board on page 170.

- Announcement fragments and announcements.

An announcement fragment is a recorded voice segment, and an announcement is a set of rules for determining when a specific fragment is to be played. For more information, see Customizing Announcements Overview on page 147.

Administration from Messaging Web Interface screens

Communication Manager Messaging is pre-configured with default settings such that an administrator does not need to manually configure a setting to be the default setting.

The legend on the Messaging Administration Web page lists the web page links. The Legend is divided in sections as per the functionality provided by each web page. For example, all administrative related web pages are listed under the Messaging Administration heading.

For detailed information, see Messaging Basics on page 34.

Administrative Access by More Than One Person

A system allows more than one person to perform the same function on the same screen, for example, adding a customer to the Voice Messaging database. However, when two people happen to be editing the same profile, only the changes made by the person who saves the screen last are written to the hard disk. The other changes are lost. Together, the Communication Manager server and messaging can have up to 49 different login accounts.

Help

Help is available at three levels:

- When you are using a computer or terminal, Help can be activated for any window, screen, or field. Use the Help key for the purpose of obtaining assistance:
  - The Help key provides general system information, navigation suggestions, and data entry overviews.
- Help can be obtained from the messaging documentation set. This set of documents contains detailed administrative and diagnostic procedures.
- When you are using a telephone, Help can be obtained by calling the remote services center, which is open 365 days a year.

Internet Messaging Administration

Internet Messaging Administration can be found under the IMAP/SMTP Administration heading. However, some fields require that an entry be made, after which the system will operate properly.

For additional information on Internet Messaging, see Administering Internet Messaging on page 285.

Administration Tasks

Task	Purpose	Page (All pages refer to Communication Manager Messaging web interface unless explicitly stated)	✔
To add privileged and non-privileged administrators.	This ensures system security and prevents unauthorized access to your messaging software.	• In the Server Administration page, under **Security** group, click **Administrator Accounts**. • To get access to Server Administration page, select **Server (Maintenance)** on the **Administration** menu of the System Management Interface.	
Define system limits.	This defines maximum capacities for such things as stored messages and message delivery lists.	• Under Messaging Administration, Limits	
Define basic features and parameters.	This defines login parameters and system time limits and transfer type, and globally activate certain features for all subscribers, such as multiple personal greetings.	• Under **Messaging Administration**, select **System Administration**.	
Administer transfer type and restrictions.	This enhances the system security by choosing the type of call transfers and coverages you will allow, on your system and restrict the call transfer to subscriber or to any extensions.	• Under **Messaging Administration**, select **System Administration**.	
Define thresholds for warnings.	This defines thresholds that determine when mailboxes get too full or disk space gets too low.	• Under Messaging Administration, Thresholds	

Table continues…

Task	Purpose	Page (All pages refer to Communication Manager Messaging web interface unless explicitly stated)	✔
	The messaging software plays a voice warning to subscribers when mailboxes get too full.		
Define Class of Service options.	This defines classes of service which you may then assign to subscribers. A class of service (COS) is a set of messaging capabilities.	• Under Messaging Administration Classes-of-Service	
Add subscribers.	This defines subscriber mailboxes to the system with the messaging software.	• Under Messaging Administration, Subscriber Management	
Create subscriber name recordings (optional).	This records the subscriber's voiced name fragment so that a caller or voice mail recipient hears the name, not the extension number, of the subscriber. You may give subscribers the capability to record their own names. This option is highly recommended.	• Messaging mailbox with announcement recording capability • Subscriber Management	
Set up community sending restrictions (optional).	This restricts groups of subscribers to whom you have assigned the same community number from sending mail to other groups or from receiving voice mail from other groups.	• Under Messaging Administration, Sending Restrictions	
Set up outcalling (optional).	This administers system-related outcalling parameters. Outcalling allows a subscriber to tell the messaging software to place calls to a specified number when the subscriber receives new messages.	• Under Messaging Administration, Outcalling Options	

Table continues…

Task	Purpose	Page (All pages refer to Communication Manager Messaging web interface unless explicitly stated)	✔
Set up a broadcast mailbox (optional).	This sets up a broadcast mailbox. A broadcast mailbox allows subscribers to send broadcast messages.	• Under Messaging Administration, Subscriber Management	
Customize system announcements and fragments (optional).	This changes the announcements that the messaging software plays automatically to fit the needs of your company.	Under Messaging Administration • Announcement Sets • Announcements Admin - Voice Fragments, Announcements • Announcements Copy	
Set up automated attendants (optional).	This creates automatic answering so that callers hear a menu of options, depending on the time of day and administered call routing. The callers then select options and transfer to other destinations by pressing touchtone buttons or dialing extensions.	Under Messaging Administration • Attendant Management - Auto-Attendant Routing Business & Holiday Schedule, Routing, Menu Tree	
Set up a bulletin board (optional).	This defines a bulletin board, which lets callers access a bulletin board to hear updated information or select messages from a menu of options.	• Under **Messaging Administration**, select **Subscriber Management**.	
Define Text-to-Speech (TTS) options (optional).	This determines what parts of text messages are converted into speech.	• Under **Messaging Administration**, select **System Administration**.	
Setting up and testing CMM Lockout Notification	The CMM Lockout Notification feature allows the CMM application to call you or another administrator whenever a subscriber mailbox or a CMM administrator login is	Steps to set up CMM Lockout notification • Under **Messaging Administration**, select **System Administration** to ensure either the SMTP	

Table continues…

Task	Purpose	Page (All pages refer to Communication Manager Messaging web interface unless explicitly stated)	✔
	locked due to excessive failed login attempts. You must create a lockout notification mailbox to receive the lockout notification message. You can also configure the outcalling for the lockout notification mailbox to call the administrator's telephone number when the mailbox is notified about a login violation.	Port or Alternate SMTP Port is enabled. • Under **Messaging Administration**, select **Outcalling Options** and ensure that outcalling is enabled. • Add a new subscriber with a name similar to Lockout to know the purpose of the mailbox. On the same page, enable Outcalling. • Login to the subscriber you just created, record a name for the subscriber and set the outcalling number to administrator's telephone. • Under **Messaging Administration**, select **System Administration** and provide the number of the mailbox you set up for Lockout Notification.	

Administration and maintenance tasks checklist

The following checklist lists tasks you do on a regular basis to keep the Communication Manager system with the messaging software operating properly.

Task	Purpose	Page (All pages refer to Communication Manager Messaging web intergace unless stated explicitly)	✔
Administer and remove subscribers, as necessary.	This maintains subscriber profiles to reflect current needs and staffing.	• Under Messaging Administration, Subscriber Management	
Reassign subscriber default password.	This reassigns a subscriber's default password if the subscriber forgets it.	• Under Messaging Administration, Subscriber Management	
Unlock a subscriber's mailbox.	This unlocks a subscriber's mailbox if too many unsuccessful attempts have been made to log in to it.	• Under Messaging Administration, Subscriber Management	
Run traffic reports.	This displays messaging traffic information to help you troubleshoot and find ways to improve system efficiency.	Under the **Server Reports** group, click **Measurements**. The following options are available: • Load Hourly or Daily Traffic • Subscriber Daily or Monthly Traffic • Remote-Messages Daily Traffic or Monthly Traffic • Network-Load Hourly or Daily Traffic • Community Daily or Daily Traffic • Feature Hourly or Daily Traffic • Special-features Daily or Hourly Traffic • Traffic-Snapshot Daily or Monthly Traffic	
Administer and check the Activity Log.	This allows you to investigate subscriber activity to resolve reported problems.	• Under Messaging Administration, Activity Log Configuration	

Table continues…

Task	Purpose	Page (All pages refer to Communication Manager Messaging web intergace unless stated explicitly)	✔
Check the Alarm Report.	This displays active or resolved messaging software alarms. You can check that alarms are cleared after service procedures are performed, and troubleshoot intermittent problems that resolve themselves and then recur.	• Under Logs, Alarm	
Check the Administration Log.	This allows you to display and investigate administrative entries that you can solve.	• To configure Subscriber Activity Log, select **Activity Log Configuration** under **Messaging Administration**. • To view Subscriber Activity Log, select **Subscriber Activity** under **Logs**.	
Run audits.	This synchronizes the system software and the disk after you have made administrative changes. Also, run audits to allow the system to readjust itself after an alarm.	Under Utilities, Messaging DB Audits. This page has provision to audit the following: • Mailboxes • Mailing Lists • Voice Names • Network Data • Subscriber Data • Personal Directory • Nightly and weekly data And also has provision to display the past audits that have run and their status in the Audit History page.	

Table continues…

Task	Purpose	Page (All pages refer to Communication Manager Messaging web intergace unless stated explicitly)	✔
Backup data on demand, and restore data if needed.	This stores backup system data immediately after a large number of changes.	• Use the Communication Manager server web browser Data Backup/ Restore options.	
Perform a Backup		Backup messaging translations data on page 303 .	
Prepare for Scheduled Backups		The time of scheduled backups should already be established. Add messaging data to the backups on page 306 .	

Basic Messaging Administration

Defining system limits

About this task

Note:

Administration and maintenance tasks checklist on page 49 contains a checklist of initial administrative tasks you can use as a guide for performing messaging administration.

Your messaging software comes with default system limits. These limits consist primarily of maximum capacities for such items as stored messages and message-delivery lists. You can change system limits at any time on the Limits page to define system capacities.

Procedure

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

   The system displays the Limits screen.
4. Type appropriate values for the fields and click **Update Limits**.

Limits field descriptions

Table 2: MESSAGE LIMITS

Field Name	Valid Input	Description/Procedure
Maximum Message Length	16 to 10800 Default: 10800 (180 minutes)	Enter the length, in seconds, of the longest message that can be created. Maximum message lengths for individual subscribers can be further restricted on the Class of Service and Subscriber screens.
Minimum Message Length	1 to 99 Default: 10	Use this field to enter the length of the shortest message that the messaging system will recognize as a message. All values must be in tenths of seconds.

Table 3: ADMINISTRATION LIMITS

Field Name	Valid Input	Description/Procedure
Local Subscribers	1000, 2400, 6000, and 15000	This field displays the maximum number of subscribers that can be administered on the messaging software system. The value is determined when you purchase or upgrade your system and can only be changed by technical support engineers.
Maximum Administered Remotes	0 to 125000	Enter the maximum number of remote subscribers that can be administered on this messaging software system.
Maximum Totals Lists	0 to 999999	Enter the total number of entries allowed in all subscribers' lists.
Maximum Lists Per Subscriber	0 to 999	Enter the maximum number of lists allowed per subscriber.
Maximum Recipients Per List	0 to 250	Enter the maximum number of entries (recipients) allowed per subscriber list.

Button	Description
Update Limits	Updates the limits that you have set.

Managing extensions

Changing Extension Numbers

About this task

Follow the below procedure to change the extension of a local or a remote subscriber:

Procedure

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

   System displays the Manage Subscribers page.
4. Click **Manage** for Local Subscribers or Remote Subscriber depending on the type of subscriber whose extension you want to change.

   The Manage Local Subscribers or Manager Remote Subscribers page is displayed
5. Select the subscriber from the list.
6. Perform one of the following action:
   - Click **Edit/Delete the Selected Subscriber** for local subscribers.
   - Click **Edit the Selected Subscriber** for remote subscribers.
7. In the **Mailbox Number** field, type the new extension.
8. Click **Save**.

Guidelines for Using the Change Extensions page

The Change Extensions page allows you to change a block of extensions for local and remote servers. To access the page, go to **Utilities** menu on the left hand panel.

Consider the following guidelines before you change extension numbers:

- To change the length of local extension numbers:

  First change the length of extensions at the platform level, using the Switch Link Administration page.
- To move numbers on the local machine:
  - This screen can move all of the covering extensions in a given range of numbers. However, it does not change references to the local system in networked systems.
  - If the system you want to change is networked to other messaging systems, you must also change the extension length for this machine in all connected systems.
  - Ports on the system with local subscribers whose extensions are to be changed are disabled while you make the necessary changes. Therefore, plan to make the changes when traffic is slow.
- To change extensions for automated attendant and ELA Shadow Mailbox:

  This screen does not change the extensions for automated attendants or ELA Shadow Mailbox. If you use this screen to change an automated attendant extension, and an automated attendant is set up to call that extension, follow the procedures in Automated Attendants and Bulletin Boards on page 170 to change the automated attendant extension manually. For setting up a mailbox, refer to Setting Up a Broadcast Mailbox on page 75.

Changing the length of extensions

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the left navigation pane, click **Switch Link Admin**.
4. In the **Extension Length**, select a value between `Variable` through `50` from the drop-down menu.

   The number must match the dial plan of the Communication Manager server.
5. Click **Save** to update the system.

Changing a Block of Extension

About this task

You may or may not choose to change the extension length before changing a block of extensions.

To change a block of extensions:

Procedure

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

   The Change Extensions page is displayed.
4. In the **Machine Name** filed, select the name of the machine on which you plan to change or add extensions.
5. If you have changed the extension length, the system displays the new extension length in the **Extension Length** field.
6. Note the ranges of extension numbers in the **Start Extension** and **End Extension** fields on the Edit Messaging Server page before you make any modifications.

   You can update a remote machine by selecting the appropriate machine name on the page.

   Tip:

   If you have a system printer, print a copy of the extension assignments before you continue.
7. In the **Old Beginning Extensions** field and the **Old Ending Extensions** field, enter the boundaries of the extension numbers you are changing.

   That is, enter two numbers: the beginning (smallest affected) extension number and the ending (largest affected) extension number.

8. In the **New Beginning Extensions** field, and the **New Ending Extensions** enter the beginning number and the ending number of the new block of numbers.
9. Click **Update Extensions**.

   The system changes the range of subscriber extensions for the selected machine.

Changing a block of extensions without changing the length of the extensions

About this task

To change a block of extensions from one series of numbers to another series of equal length:

Note:

The Change Extensions page affects many other settings on local and remote networked messaging systems. Use this page only after you carefully plan the changes you want to make.

Procedure

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

   You can change a block of extensions on the Change Extensions page

   Note the ranges of extension numbers in the **Beginning Extension** and **Ending Extension** fields before you make any modifications.

   Important:

   You must busy all voice and networking ports before beginning the change extension operation, and release them after the operation is complete.
4. For Remote systems, select the desired machine from the **Machine Name** field. If you want to change its block of extensions, define the intended new block of extensions.
5. In the **Machine Name** field, click the name of the Communication Manager Messaging server on which you are changing extension numbers for local subscribers.

   This is the only system on which you perform this procedure.
6. In the **Old Beginning Extensions** field and the **Old Ending Extensions** field, enter the boundaries of the extension numbers you are changing.

   Enter two numbers: the beginning or smallest affected extension number and the ending or largest affected extension number.
7. In the **New Beginning Extensions** field, and the **New Ending Extensions** enter the beginning number and the ending number of the new block of numbers.
8. Release the voice ports on the local system.

   The local system automatically updates any remote system with the extension number changes.

Note:

If a remote system is not administered to receive automatic updates, you can request for an update. In the **Server Administration** section, click **Request Remote Update**.

The Request Remote Update page displays the status of the request.

Change Address Range

About this task

After you decide the new extension block, you can edit the address range for the local server or a remote server.

To edit the address range:

For Local Server, go to Server Administration and click Messaging Server Admin link. The Edit Messaging Server page is displayed.

For Networked Server, go to Server Administration and click Networked Servers. The Edit Networked Server page is displayed.

Procedure

1. Re-enter the prefixes and the start and end extensions as you want them when the conversion is completed.
2. Busyout the local voice ports.
3. Release all voice ports from the busy condition.

Defining Basic Features and Parameters

About this task

The messaging software comes with default login parameters and default system time limits. Also, certain features that must be activated globally for all subscribers (for example, Multiple Personal Greetings) are either activated or not activated by default. You might want to change some of these parameters or to activate or deactivate features as the needs of system subscribers change.

To change system features and parameters:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. On the left hand panel, under **Messaging Administration** group, click **System Administration** to administer system feature parameters.

   The system displays the **Administer System Attributes and Features page**.
4. The following features can be administered:
   - Log-In Parameters
   - Subscriber Password Aging Limits (SECONDS)

- Input Time Limits (Days)
- Disconnect Options
- Miscellaneous Parameters
- Feature Activation
- Multimedia Parameters
- Call Transfer Out of Messaging
- Announcement Sets
- Rescheduling Increments for Full Mailbox Delivery

5. Click **Save**.

Administer System Attributes and Features field descriptions

Name	Valid Input	Description
LOG-IN PARAMETERS		
Login Retries	3	The number of sequential login attempts that is allowed before the messaging software disconnects the caller.
Consecutive Invalid Login Attempts	Default: 18	The maximum number of consecutive unsuccessful login attempts that is allowed before the caller is locked out of the messaging software.
Minimum Password Length	1 to 15 Default: 1	The minimum number of characters that is required for a subscriber password. Passwords should to have at least 5 digits and should exceed by at least one digit the number of digits in an mailbox number. If limitations are not in place, many subscribers often choose easily guessed numbers for their password.
Passwords History	From 0 to 15	The number of unique new passwords a user must use before an old password can be reused.
Lock Duration	0, 5 to 7200	The time duration (number of minutes) that a mailbox account is locked after a subscriber fails to login before unlocking automatically. The default value 0, indicates that Messaging does not automatically unlock a mailbox.
Lockout Notification Mailbox		The mailbox number, where a locked login notification will be sent. When a local mailbox gets locked, it sends out a notification message to the Lockout Notification Mailbox number.
System Guest Password	From 1 to 15 numeric characters	A password that people without mailboxes can use to leave messages for system subscribers.

Table continues…

Name	Valid Input	Description
	Default: blank	The system does not allow subscribers to create a password that is the same as the guest password.
PASSWORD AGING LIMITS (DAYS)		
Password Expiration Interval:	From 1 to 999 Default: 0; turns password aging off	The number of days that a password is active for the messaging software. • The valid values are from 0 to 999. • The default value is 0 indicating that password expiration is disabled. The value in this field, must be greater that the sum of the **Minimum Age Before Changes** field and the **Expiration Warning** field.
Minimum Age Before Changes	From 0 to 99 Default: 0	The minimum number of days that must pass before subscribers can change their passwords again after a successful change.
Expiration Warning	From 0 to 99 Default: 0	The number of days before the password expires for the system to notify the subscriber of impending expiration. If you enter **0**, a subscriber does not receive any warning that the password is about to expire.
INPUT TIME LIMITS (SECONDS)		
Normal	Default: 60	The number of seconds to wait for a subscriber to enter a command before sending a timeout warning.
Full Mailbox Timeout	Default: 5	The number of seconds to wait for a touchtone entry from a caller after informing the caller that the called subscriber's mailbox is full.
Wait (*W)	Default: 180	Enter the number of seconds to wait after a subscriber enters the wait command (*** W** or *** 9**) before sending a time out warning.
Between Digits at Auto-attendant or Standalone Menu	Default: 3	The maximum number of seconds the messaging software waits between touchtone signals before timing out. If a caller does not press another key, the system is disconnected. This maximum applies both to interaction with an automated attendant menu and to touchtone signals during a call answer session, for example, during the time a caller is to enter a destination extension.
DISCONNECT OPTIONS		
Quick Silence Disconnect	yes no	Enables or disables quick silence disconnect.

Table continues…

Name	Valid Input	Description
	Default: no	Quick silence-disconnect signaling enhances messaging operation for calls in which there is no disconnect signaling and the line simply goes silent after the caller hangs up. When quick silence disconnect is administered, the system is disconnected as follows: • During a call answer recording, upon detecting silence for a period that exceeds the silence limit administered on this screen. • At all other times, after two expirations of the Input time limit (see INPUT TIME LIMITS (SECONDS) on page 58). The messaging software provides a system prompt and a Help message after the first expiration. The system says "Goodbye" and is disconnected after the second expiration. When recording a message in a voice mail session (as opposed to a call answer session), the system is not disconnected upon detecting silence but rather after two expirations of the input time limit. If you use quick silence disconnect, there are long periods of silence at the end of call answer messages. If subscribers report problems with the silence in messages, consider changing this setting.
Silence Limit	From 5 to 30 Default: 30	The time in seconds to wait for caller input before dropping call answer recordings if quick silence disconnect is enabled.
Miscellaneous Parameters		
Broadcast Mailbox Extension	Default: blank	The extension number of the system broadcast mailbox.
System Prime Time, Start: End:	24-hour clock time in the format hh:mm Defaults: Start = 8:00 End = 17:00	The starting time for the prime-time interval for traffic collection and multiple personal greetings. (This is normally the time that your company opens for business.) The ending time for the prime-time interval for traffic collection and multiple personal greetings. This is normally the time that your company is closed.
Increment (l/s), Rewind: Advance:	Short (4 sec) Long (10 sec) Default: Short (4 sec)	Sets the rewind and advance amounts to 4 seconds. **l** sets the amounts to 10 seconds.

Table continues…

Name	Valid Input	Description
		These values are used when a subscriber wants to: • Repeat the previous few seconds of the message (press **5**). • Advance the message (press **6**).
Maximum Simultaneous LDAP Directory Update Sessions	Default: 100	The maximum simultaneous LDAP sessions during a full remote update. When the maximum is reached, an administrator cannot request a full remote update until one of the sessions is finished.
Anonymous LDAP Authentication	Authenticated Only Authenticated or Anonymous	Enables or disables the Anonymous LDAP Authentication. Anonymous LDAP Authentication allows end users to access the CMM directory to obtain, mailbox number or CMM email address, in order to address a message using a starndards based email client such as Outlook.
Default Internet Subscriber community	1 to 15 Default: 1	The default community assigned to subscribers external to the system. These internet subscribers include all email addresses not known by the system as local or remote subscribers.
Feature Activation		
Traffic Collection	yes no Default: yes	Enables or disables the collection of traffic data.
Privacy Enforcement Level	Voice Email Default: Voice	The type of privacy enforcement. Whether it is the Voice style privacy or Email style privacy. **Note:** Message forwarding of private messages is never available from the TUI. If you select **Voice**, messages will only be delivered or available to clients that are known to respect voice-mail style privacy. Most email clients (e.g. IMAP4, POP3) do not restrict the forwarding of messages. If you select **Email**, the message will be marked as private and it will be up to the recipient to enforce the privacy of the message when using a standards based email client.

Table continues…

Name	Valid Input	Description
Name Record by Subscriber	yes no Default: yes	Allows or disallows subscribers to from recording their own names.
Automatic Mail Forwarding	yes = allowed no = not allowed private = allowed according to privacy level. Default: yes	Allows or disallows Automatic Mail Forwarding. If you select yes, private messages will be forwarded regardless of the Privacy Enforcement Level. If you select private, private messages will be forwarded according to the Privacy Enforcement Level. Messages that are blocked will be left in the mailbox regardless of whether delete after forwarding is selected.
Multiple Personal Greetings	yes no Default: yes	Enables or disables the Multiple Personal Greetings feature. The Multiple Personal Greetings feature is applied to the entire system.
End of Message Warning	yes no Default: yes	Enables or disables the End of Message Warning feature.
End of Message Warning	Default: 15 0 = no warning	The number of seconds before the end of the allotted message recording time, when the End of Message Warning prompt plays.
Priority on Call Answer	yes no Default: yes	Allows or disallows callers to designate a call answer message priority. Callers can designate the message as private, regardless of this setting.
Call Answer Disable	yes no Default: no	Allows or prevents subscribers to disable call answer. If activated, callers hear the subscriber's greeting but cannot leave a message. Subscribers are addressed to record appropriate instructions in their personal greetings so that callers can understand the options.
Address Before Record	yes no Default: no	Enables or disables the system to prompt subscribers to address a message before recording. Subscribers who ignore the prompt can still edit the address list after they create the message.

Table continues…

Name	Valid Input	Description
Calling Party Number	yes no Default: no	Enables or disables external calling party numbers if they are available from the Communication Manager.
MULTIMEDIA PARAMETERS		
Text to Speech Conversion (TTS):	None Headers Only Headers and Bodies	Determines which portions of a message containing text the system converts to speech. If you select **Headers Only**, TTS will be used for header items only. TTS is used to speak items within the message headers. Some examples would be the subject, or the sender's name. If you select **Headers and Bodies**, TTS will be used for all text components. TTS is used to speak text items within message headers as well as the text component of the message body. If you select, **None**, No TTS will be used.
CALL TRANSFER OUT OF MESSAGING		
Transfer Type	None Enhanced Cover 0 Enhanced No Cover 0	Determines if the Call Transfer Out of Messaging feature is active, and the type of enhanced call transfer is used. Enhanced Cover 0, follows the coverage path for the covering extension and Enhanced No Cover 0, does not follow the coverage path for the covering extension. None, no call transfer is allowed. However, you can press `*T` to transfer the call to another extension.
Transfer Restriction	Subscribers Digits Default: Subscribers	The restriction on calls that are to be transferred out of Messaging using "*T"(*8). Calls are transferred based on the specified restriction criteria. This field works in conjunction with the Transfer Security function. **Caution:** This feature may allow Toll Fraud and must be enabled with that in mind.
Covering Extension	Default: blank	The default extension to which a caller will be transferred when they press `0` or `*0` to transfer out of the Messaging system.
ANNOUNCEMENT SETS		

Table continues…

Name	Valid Input	Description
System	Default: us-eng	The announcement set used for system prompts.
Administrative	Default: blank	The announcement set that is used when modifying announcement fragments and composition.
SYSTEM TCP/IP PORTS		
LDAP Port	Enable Disable	The state of the primary LDAP port. Changing the state of the LDAP port temporarily interrupts the external access to LDAP. The default port number is 389 and the port number is not editable.
LDAP SSL Port	Enable Disable	The port number of the LDAP SSL port. By default the LDAP SSL port is enabled. Changing the state of the LDAP SSL port temporarily interrupts the external access to LDAP. The default port number is 636.
LDAP Front End Alternate Port	Disable	The secondary port for LDAP. This port is optional. By default the port is disabled. You cannot change the status of this port. The port is automatically enabled when you enter a port number. The default status of the port is blank.
LDAP Directory Update Port	Disable	The port that the directory update LDAP server uses for directory updates from other Messaging servers in the network. By default the port is enabled. You cannot change the status of this port. The default port number is 56389.
Internal System IMAP4 Port	Enable	The internal System IMAP4 port. By default the port is enabled. You cannot change the status of this port. It is recommended that you leave this field at the default value. The default port number is 55143.
IMAP4 Port	Enable Disable	The port that IMAP4 clients use for IMAP4 connectivity.

Table continues…

Name	Valid Input	Description
		If you click **Enabled**, type the port number that the IMAP4 server will use. The default port number is 143.
IMAP4 SSL Port	Enable Disable	The port that IMAP4 clients use for IMAP4 SSL connectivity. If you click **Enabled**, type the port number that the IMAP4 server will use. The default port number is 993.
POP3 Port	Enable Disable	The port that POP3 clients use for POP3 connectivity. If you click **Enabled**, type the port number that the POP3 server will use. The default port number is 110.
POP3 SSL Port	Enable Disable	The port that POP3 clients use for POP3 SSL connectivity. If you click **Enabled**, type the port number that the POP3 server will use. The default port number is 995.
SMTP Port	Enable Disable	The port that SMTP clients use for SMTP connectivity. If you click **Enabled**, type the port number that the SMTP server will use. The default port number is 25.
SMTP Alternate Port	Enable Disable	The port that SMTP clients use for SMTP connectivity. This is an additional port that can be used on the public network instead of the traditional SMTP port. The port is automatically enabled when you enter a port number. By default, this port is disabled and the port number is blank. The default status of this port is blank.
SMTP SSL Port	Enable Disable	The port that SMTP SLS clients use for SMTP SSL connectivity. If you click **Enabled**, type the port number that the SMTP server uses for SMTP SSL communication. The default port number is 465.

Table continues…

Name	Valid Input	Description
Allow TLS for Outgoing SMTP	Enable Disable	The option to enable TLS on the outgoing SMTP port that encrypts the SMTP conversation. By default, TLS on outgoing SMTP is enabled. The default port number is 25.
MCAPI Port	Enable	The port that the MCAPI server uses. If you change the port number, you must restart the system. The default port number is 55000.
RESCHEDULING INCREMENTS FOR FULL MAILBOX DELIVERY		
Increment_<n>		The incremental interval in days, hours, and minutes during which the system waits to resend messages. When the mailbox is full, the system waits and resends the messages according to the incremental interval. When the system reaches a zero increment, the system does not deliver messages. You can specify maximum 10 rescheduling increments to reattempt delivery of a message to a full mailbox.

Enabling automatic mail forwarding

About this task

With Communication Manager Messaging, you can forwards mails to:

- Microsoft Exchange
- An external SMTP account, such as Yahoo! or Gmail
- Another user

To prevent unwanted automatic traffic, by default, mail forwarding is disabled.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **System Administration**.
4. In the **Automatic Mail Forwarding** field, click one of the following options:

Choice Option	Choice Description
yes	If you select **yes**, private messages will be forwarded regardless of the Privacy Enforcement Level.

Choice Option	Choice Description
no	If you select **no**, Mail Forwarding is not allowed.
private	If you select **private**, private messages will be forwarded according to the Privacy Enforcement Level. Messages that are blocked will be left in the mailbox regardless of whether delete after forwarding is selected.

5. Click **Save**.

Controlling Call Transfers

This topic describes how to add or deny transfers to certain numbers out of the messaging software and how to enable transfers to others.

Factors to consider when planning Call Transfer Controls

The **Call Transfer Administration** gives you control over call transfers and helps you to prevent toll fraud. You can also use **Call Transfer Administration** to specify extensions to which a caller is permitted to transfer.

Callers cannot transfer to numbers expressly denied. For example, you may want to forbid call transfer to numbers beginning with 9 if this number accesses an outside line.

Denied numbers override numbers not specified on these pages. Allowed numbers override numbers specifically denied. For example:

If you used the Denied Number Addition to	and you used the Allowed Number Addition to	then a caller can
deny all numbers	allow numbers in the range from 2000 to 5999	transfer out of the messaging software by dialing any 4-digit number that starts with 2 to 5.
deny all numbers	allow a specific number	transfer only to that number, for example, a remote field office.

To deny all numbers, type `all` in the **From** field of the Add Denied Transfer Numbers page and leave the **To** field blank. You can use a similar method to enter a single number (rather than a range) in either the Add Denied Transfer Numbers page or the Add Allowed Transfer Numbers page. Simply enter the number you need into the **From** field of the applicable page.

Adding Allowed Transfer Numbers

About this task

Use the **Allowed Number Addition** to specify allowed transfer numbers, that would otherwise be denied, because the numbers are included in the denied transfer numbers.

Note:

If denied transfer numbers contain the entry `all`, then you can only transfer to those numbers that appears on the **Allowed Number Display** page.

If denied transfer numbers does not contain the entry `all`, then you can transfer to any number.

Procedure

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

   System displays the Add Allowed Transfer Numbers.
4. Do one of the following:

   - Type a starting extension in the **From** field and an ending extension in the **To** field to allow a range of numbers. Most administrators choose to deny all transfers and then use this page to specify the few numbers or classes of numbers that do not affect system security.

   For example, enter 4000 in the **From** field and 5999 in the **To** field to allow 4-digit transfers to any numbers between 4000 and 5999.

   - Enter **all** in the **From** and **To** fields to allow all transfers.

   Note:

   No two allowed transfer entries can overlap each other. For example, you cannot make an entry to allow transfer numbers between 4000 and 5999 and then make another entry to allow transfer numbers between 5000 and 6999. Instead, enter one range of from 4000 to 6999.
5. Click **Save** to save the information in the system database.
6. Do the step 3 through 5 again, to add other allowed transfer numbers.

Next steps

Go to **Allowed Number Display** to view the list of allowed transfer numbers you have added.

Deleting Allowed Transfer Numbers

About this task

Use the **Allowed Number Deletion** to remove entries from the allowed transfer numbers database.

Procedure

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

   The system displays the Delete Allowed Transfer Numbers page.
4. You can delete either a single number or a range of numbers. Perform one of the following actions:

   - If you want to delete a single number, then type the number in the **From** field and left the **To** field blank.

- If you want to delete a range of numbers, then type the starting extension of the range, in the **From** field and the ending extension in the **To** field.

5. Click **Delete**.

Next steps

Go to **Allowed Number Display**, to ensure that you have deleted the correct number or the range of numbers.

Displaying Allowed Transfer Numbers

About this task

You can display allowed transfers numbers. This page displays the entries in the allowed transfer numbers database.

Follow the below procedure to view the allowed transfer numbers:

Procedure

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

Result

The system displays the Display Allowed Transfer Numbers page.

Adding Denied Call Transfer Numbers

About this task

Use the **Denied Number Addition** to specify numbers to which transfers are to be denied. To add denied transfer numbers:

Procedure

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

   The system displays the Add Denied Transfer Numbers page.

4. Do one of the following:

   - Type `all` in the **From** field to deny all transfers. Most administrators choose to deny all transfers, and then allow a few numbers or classes of numbers that do not affect system security.
   - Enter a starting extension in the **From** field and an ending extension in the **To** field to deny a range of numbers.

For example, enter 4000 in the **From** field and 5999 in the **To** field to restrict 4-digit transfers to any numbers between 4000 and 5999.

Note:

No two restricting entries can overlap each other. For example, you cannot enter a restriction to any numbers between 4000 and 5999 then enter another restriction between 5000 and 6999. Instead, enter one range of 4000 to 6999.

5. Click **Save** to save the information in the system database.
6. Do the step 3 through 5 again, to add other denied transfer numbers.

Next steps

Go to **Denied Number Display** to view the list of denied transfer numbers you have added.

Deleting Denied Transfer Numbers

About this task

Use the **Denied Number Deletion** to delete entries from the denied transfers numbers database.

Procedure

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

   System displays the Delete Denied Transfer Numbers page.
4. You can delete either a single number or a range of numbers. Perform one of the following actions:
   - If you want to delete a single number, then type the number in the **From** field and left the **To** field blank.
   - If you want to delete a range of numbers, then type the starting extension of the range, in the **From** field and the ending extension in the **To** field.
5. Click **Delete**.

Next steps

Go to **Denied Number Deletion**, to ensure that you have deleted the correct number or the range of numbers.

Displaying Denied Transfer Numbers

About this task

You can display denied transfers numbers. This page displays the entries in the denied transfer numbers database.

Follow the below procedure to view the denied transfers numbers:

Procedure

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

Result

The system displays the Display Denied Transfer Numbers page.

Defining Thresholds for Warnings

About this task

The messaging software plays a warning message to subscribers when their mailboxes reach the threshold limits specified on the Thresholds page. You can change these thresholds as the use of your system changes.

To change the system thresholds:

Procedure

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

   The system displays the Thresholds page.
4. In the **Lower Threshold** field, type the minimum message space threshold for a subscriber mailbox.

   Valid values are `0` through `100`.
5. In the **Upper Threshold** field, type the maximum message space threshold for a subscriber mailbox.

   Valid values are `0` through `100`.
6. Click **Update Thresholds** to save the changes.

Thresholds field descriptions

Field Name	Valid Input	Description/Procedure
SUBSCRIBER MESSAGE SPACE WARNING		
Lower Threshold:	0 to 100 Default: 50	The lower threshold for the message space in a subscriber's mailbox. This value is a percentage of the subscriber's mailbox space. When this

Table continues…

Field Name	Valid Input	Description/Procedure
		threshold is reached, a warning message is issued to the subscriber upon login to his or her mailbox. Recommended values are 50% for small mailboxes (less than 9 minutes) and 80% for larger mailboxes.
Upper Threshold:	0 to 100 Default: 80	The upper threshold for the message space in a subscriber's mailbox. This value is a percentage of the subscriber's mailbox space. When this threshold is reached, a warning message is issued to the subscriber upon login to his/her mailbox. Recommended values are 80% for small mailboxes (less than 9 minutes) and 95% for larger mailboxes.

Setting Up Community Sending Restrictions

About this task

A community is a group of subscribers to whom you have assigned some type of calling restrictions. The administration of communities enables you to further define the allowed call destinations of your subscribers.

You create a community to prevent members from:

- Sending mail to other groups
- Receiving mail from other groups

For example, imagine that you have just set up two communities. Community 1 cannot send messages to international communities. Therefore, you assign the subscribers who cannot have international access to Community 1. Community 2 has international access. Therefore, you assign the international machines and the individuals who are permitted to access international numbers to Community 2.

Then you administer the communities so that Community 1 is restricted from sending messages to Community 2. This process tells the messaging software which subscribers can and cannot access international destinations.

To set up sending restrictions between communities:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.

2. On the **Administration** menu, click **Messaging**.
3. In the left navigation pane, under the **Messaging Administration** group, click the **Sending Restrictions**.

   The system displays the Edit Sending Restrictions page.
4. Use the checkboxes to establish sending restrictions between communities of subscribers.

   If a box is checked, the corresponding sender community (row) cannot send voice mail to members of the corresponding recipient community (column).
5. Click Save.

Setting Up Outcalling

About this task

The Outcalling feature allows a subscriber to tell the messaging software to place a call to a specified number when the subscriber receives new messages. Use the Outcalling Options page to administer the outcalling options used by the Messaging feature.

Security alert:

Use of the outcalling feature greatly increases the risk of toll fraud. You must specify a maximum number of outcalling digits that is as small as possible. You also need to take precautions by placing additional restrictions on the messaging outcalling ports, other messaging ports, trunk access codes, and so on. See Security on page 251 for more information.

To set up outcalling parameters:

Procedure

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

   The system displays the Outcalling Options page.
4. Type appropriate values for the fields and click **Update Features** to save the changes.

   Note:

   After you have set up outcalling, you must also assign outcalling permission to each subscriber you want to be able to use the feature. For more information, see Subscriber Administration on page 91.

Outcalling Options field descriptions

Field Name	Valid Input	Description/Procedure
Outcalling Active	Yes No	Enables or disables outcalling on a system wide basis. **Note:** This feature uses voice ports.
Start Time	24-hour clock time in the format hh:mm Default: 00:00 (midnight)	The beginning of the time period during which outcalling can occur. You can specify up to three time periods. These time periods cannot overlap and the sum of their durations must be less than 24 hours.
End Time	24-hour clock time in the format hh:mm	The end of the time period during which outcalling can occur. You can specify up to three time periods. (See Start Time above.)
Interval	24-hour clock time in the format hh:mm	The time interval between outcalling attempts within the time period during which outcalling is permitted. The default value for the first time period is 00:15 (15 minutes). The minimum interval is 15 minutes. The maximum is 24 hours.
Maximum Simultaneous Ports	1 to 64 Default: 1	The maximum number of voice ports that you can use simultaneously for outcalling during this time period. The maximum simultaneous ports are not dependent on the time slot.
Initial Delay (mins):	0 to 60 Default: 0	The number of minutes that pass after the delivery of a message before the messaging software makes the first outcall.
Maximum Number Digits:	3 to 60 Default: 29	The maximum number of button-presses (including digits and the symbols * and #) that the subscriber can specify for outcalling. You can limit digits so that subscribers cannot use outcalling

Table continues…

Field Name	Valid Input	Description/Procedure
		to place off-premises or long distance calls.

Broadcast Messages

A broadcast mailbox allows subscribers to send broadcast messages and record login announcements. You must set up a specific broadcast mailbox to store the broadcast messages.

All login announcements and broadcast messages are stored in the broadcast mailbox. When subscribers listen to a login announcement, the system retrieves the announcement from the broadcast mailbox. But when subscribers listen to a broadcast message, the system links the broadcast message to the subscriber's mailbox from the broadcast mailbox.

The broadcast mailbox can contain a maximum of 16 broadcast messages and one login announcement.

Setting Up a Broadcast Mailbox

About this task

Follow the below procedure to set up a broadcast mailbox:

Procedure

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

   The system displays the Manage Subscribers page.
4. In the **Local Subscriber Mailbox Number** field, type a new mailbox number and click the **Add or Edit**.

   Use a mailbox number that is not administered on the switch.
5. In the BASIC INFORMATION section, perform the following actions:
   a. In the **Last Name** field, type the last name of the broadcast mailbox.
   b. In the **First Name** field, type the first name of the broadcast mailbox.
   c. In the **Class Of Service** field, select the class of service name or number you want for this broadcast mailbox.
   d. In the **MWI Enabled** field, select **no** from the drop-down list.
   e. In the **Broadcast Mailbox** field, select **yes** from the drop-down list.
6. In the PERMISSIONS section, perform the following actions:
   a. In the **Type** field, select **none** from the drop-down list.
   b. In the **Broadcast** field, select **none** from the drop-down list.

7. In the INCOMING MAILBOX section, perform the following actions:
   a. In the **Retention Time, New** field, type maximum number of days, that you want a new broadcast messages to remain in the incoming mailbox.
   b. In the **Retention Time, Old** and **Retention Time, Unopened** fields, type the same number of days, as typed in the **Retention Time, New** field.
8. In the MISCELLANEOUS section, perform the following action:

   In the **Mailbox Size (seconds), Maximum** field, type the maximum number of seconds of mailbox space, that you want to assign for the broadcast mailbox.

   A valid entry is a number from `0` through `32767`.

   Make sure that you enter enough time for all the messages you believe your system will need to store at one time.

   Note that the maximum message length for a broadcast message varies, depending on the maximum message length administered for the specific subscriber who is creating a broadcast message.
9. Click Save.

Creating a Broadcast Message

A broadcast message is a message that you send to all messaging subscribers on a Communication Manager server. It is treated as a new message and is presented before normal messages. Broadcast messages are useful for company announcements or emergency announcements.

You create and send a broadcast message normally, except you do not address it. Instead, you mark the message as a broadcast message. You cannot send a broadcast message to subscribers on other systems or at other locations.

Guidelines for Broadcast Messages

Turn on message notification only in emergencies. The system slows down significantly when many subscribers simultaneously try to get a broadcast message.

Administer the broadcast mailbox so that the system deletes the message from the broadcast mailbox when the message expires.

With a 2-day default expiration, subscribers can receive the message for up to 3 days, that is, during the day you send it and the next 2 days. After the third day, the message can no longer be accessed.

If the broadcast mailbox already has 16 active broadcast messages, your message is immediately categorized as nondeliverable.

Sending a Broadcast Message

Procedure

1. Log in to your mailbox.
2. Press `1` to record a message.

3. Record, edit, and address a message.
4. Press `8` to mark the message as broadcast.

   If a subscriber cannot mark a message as broadcast, the subscriber does not currently have permission to send broadcast messages. To allow a subscriber to send broadcast messages, go to the Edit Local Subscriber page and enter `voice` in the **Broadcast** field.
5. (OPTIONAL) Press any of the following:

1	Make private. (Press 1 again to undo.)
3	Schedule delivery.
4	File a copy.

   Note:

   A broadcast message cannot be a priority message.
6. (OPTIONAL) Press `* M` to access the following additional options:

1	Turn on the message waiting indicator . (Press 1 again to undo.)
2	Change the message expiration from the 2-day default: a. Enter numbers for the month and day of expiration. For example, press 1 0 0 8 for October 8. **Note:** The month can consist of either 1 or 2 digits. The day must consist of 2 digits. b. Press `#` to save the expiration date or press `2` to start over.
#	Approve additional options.

7. Press `#` to approve your message.

Sending Login Announcements

A login announcement is a voice mail message that automatically plays to each subscriber when the subscriber logs into his or her mailbox.

Guidelines for Login Announcements

Login announcements have the following special characteristics. They:

- Do not turn on message-waiting indicators. Therefore, do not use login announcements for emergencies.
- Are not put in subscribers' mailboxes. Subscribers cannot delete, save, replay, or forward login announcements. Thus, the only way to replay login announcements is to log in again.
- Can be active only one at a time.

- Do not activate outcalling.
- Do not show up on TeleTypewriter (TTY) systems. Therefore, a hearing-impaired subscriber who uses only TTY for messaging does not see them. Send TTY subscribers a mail message from a TTY instead.
- Go to all subscribers of the system. Therefore, be sure to record all login announcements in all languages used.

Making a message a login announcement

Procedure

1. Log in to your mailbox.

   See the process flowchart Figure Login Announcement Operation on page 79.

2. Press `1` to record a message.
3. Press `# #` to approve the message.
4. Press `9` to mark the message as a login announcement.

   If a subscriber cannot mark a message as a login announcement, that subscriber does not currently have permission to send login announcements. To allow a subscriber to send login announcements, go to the Edit Local Subscriber page and type `login` in the **Broadcast** field.

   If the broadcast mailbox already holds a login announcement that is not yet expired, the messaging software informs broadcasters that new login announcements are non deliverable.

   Note:

   A login announcement cannot be marked as a private or priority message.

5. (OPTIONAL) Press:

3	Schedule delivery.
4	File a copy.

6. (OPTIONAL) Press `* M` to access the following additional options:

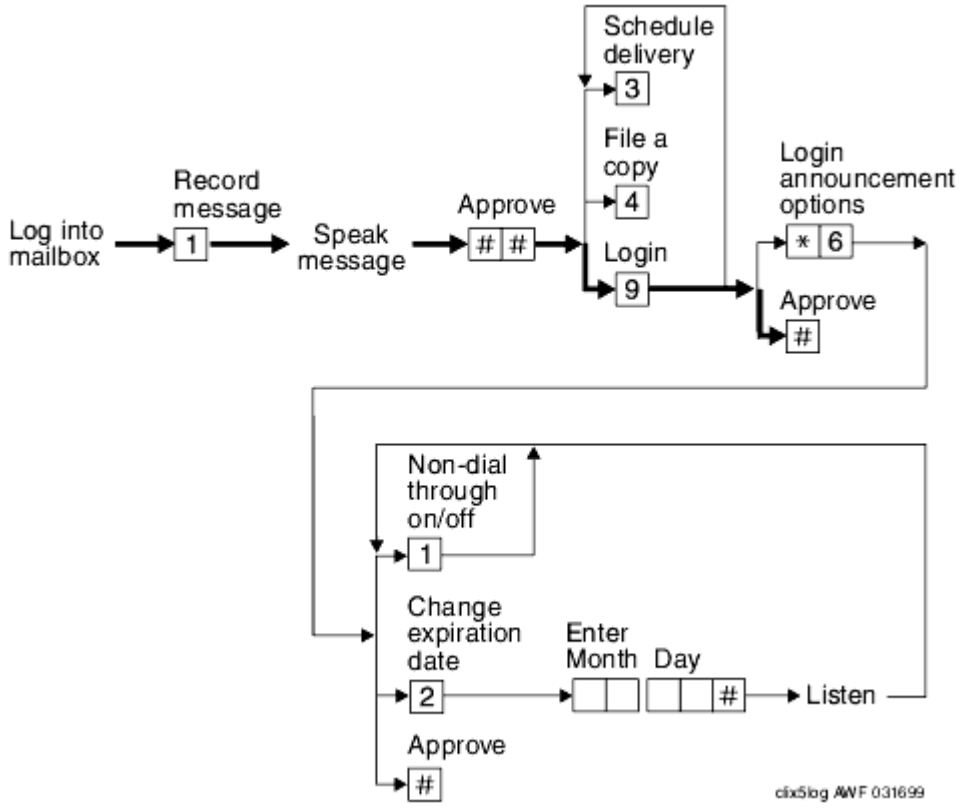
1	To turn off dial-though capability. (Press `1` again to undo.) **Note:** Turning off dial-through ensures that subscribers hear the entire announcement when logging in.

Table continues…

2	Change the message expiration from the 2-day default: a. Enter numbers for the month and day of expiration. For example, press `1 0 0 8` for October 8. **Note:** The month can consist of 1 or 2 digits. The day must consist of 2 digits. b. Press `#` to save the expiration date or press `2` again to start over.
#	Approve additional options.

7. Press `#` to approve your message.

Figure: Login Announcement Operation



The bold line shows the simplest, most direct path.

Setting up and testing CMM Lockout Notification

About this task

The CMM Lockout Notification feature allows the CMM application to call you or another administrator whenever a subscriber mailbox or a CMM administrator login is locked due to excessive failed login attempts. To set up this feature, you must create a lockout notification mailbox that uses outcalling to call the administrator's telephone number when the mailbox is notified about a login violation.

Note:

This lockout notification mailbox does not need to be associated with an extension on the Communication Manager server. This mailbox receives a text message every time a Linux login or mailbox login is locked out.

Procedure

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

   The system displays the Internet Messaging: General Options and Settings page.
4. Verify that the **Maximum number of INCOMING SMTP sessions** field and the **Maximum Number of OUTGOING SMTP Sessions** field value, is greater than `0`.
5. In the left navigation pane, under the **Messaging Administration** group, click **System Administration**.

   The system displays the Administer System Attributes and Features page.
6. Ensure the **SMTP Port** or **SMTP Alternate Port** is enabled.
7. In the left navigation pane, under the **Messaging Administration** group, click **Outcalling Options**.

   The system displays the **Outcalling Options** page.
8. In the **Outcalling Active** field, select **Yes** from the drop-down list.
9. Click **Update Features**.
10. In the left navigation pane, under the **Messaging Administration** group, click **Subscriber Management**.

    The system displays the Manage Subscribers page.
11. In the **Local Subscriber Mailbox Number** field, type an unused mailbox number and click **Add or Edit**.

This mailbox does not need to be associated with an extension on the Communication Manager server. This mailbox receives a text message every time a Linux login or mailbox login is locked out.

12. In the **Last Name** field, type `Notification` and in the **First Name** field, type `Lockout` or a similar name to notify the user at login about the purpose of the mailbox.
13. In the **Password** field, enter the password for the lockout notification mailbox.
14. Scroll down on the screen to the **Outcalling** field.
15. In the Outcalling field, select **yes**.
16. Click the **Save** button.
17. In the left navigation pane, under **Messaging Administration**, click **System Administration**.

    The system displays the Administer System Attributes and Features screen.
18. In the **Lockout Notification Mailbox** field, type the Lockout Notification mailbox number as typed in step 11.
19. Click **Save**.

Testing CMM Lockout Notification

Procedure

1. Call the messaging hunt group telephone number and login to the mailbox you just created.
2. Perform the following steps:
   a. Record a name for the mailbox, for example, "Lockout Notification”.
   b. Change the mailbox password, if prompted
   c. Press 6, then press 1 to set the outcalling number.
   d. Enter the telephone number the system should call with a lockout notification.

      Press #.
   e. Enter 9 (y) to turn on outcalling.
   f. Enter 1 to turn on for all new messages.
   g. Hang up the telephone.
3. Call the messaging hunt group extension.
4. Use an incorrect password to log into a test subscriber mailbox (not the outcalling mailbox).
5. Repeat step 4 as many times as specified in the Consecutive Invalid Attempts field on the System Administration screen.
6. Check to see if the system calls the outcalling number you entered in step 2d.

System administration

Verifying System Installation

About this task

To troubleshoot system problems, you can verify system installation to confirm that the system's primary software packages have been properly installed. The system information is displayed on the Verify System Installation page.

The Verify System Installation page confirms that the system's primary software packages are properly installed and verifies that a complete version of each application-specific package exists on the system. The system takes a few minutes to perform a series of background checks on the system software. The contents of each installed executable or help file, but not data files, are checked to verify they were unchanged during the lifetime of the system. Each of the primary software packages installed on the system is listed. Exceptions are noted in the output of this command.

To access and verify system installation:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Software Management** section, click **Software Verification**.

Result

The system verifies and lists details of the messaging application installed on the system.

Verifying system status

About this task

Based on your system configuration for messaging, the Server Status page displays information such as:

- Status of each software module
- Status of voice system
- Number of ports purchased
- Number of ports in service
- Status of networking, if applicable
- Hours of speech available
- Hours of speech used

To access and verify the system status:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Information** section, click **System Status**.

   The system displays the Server Status page.

Result

The system takes a few minutes to run checks on the status of the system and then displays the results on the page.

Interpreting the results of system status

The Communication Manager Messaging software is made up of many individual software modules. When you access the System Status page, the system requests each module to report on its status. Depending on the features you purchased, the modules that you see on the System Status page can vary from those in the table.

System Status of (Module)	Verifications	Result displayed
VM (Voice Messaging)	Messaging	IN SERVICE/ OUT OF SERVICE
ela	Enhanced list software	Running/Not running
iim	Internet messaging	Running/Not running Percent of media space in use (contains queues) Number of incoming messages in queue Number of outgoing messages in queue Number of SMTP receive sessions running Number of SMTP send sessions running Number of POP3 sessions running Number of IMAP4 sessions running Messages in SMTP queues (defer/active/incoming)
LDAP	LDAP processes	LDAP internal server: UP/DOWN LDAP front end server: UP/DOWN LDAP Corporate LAN server: UP/DOWN
	Corporate LAN LDAP access	LDAP authenticated access on the Corporate LAN: UP/DOWN LDAP anonymous access on the Corporate LAN: UP/DOWN

Table continues…

System Status of (Module)	Verifications	Result displayed
mtce (maintenance)	File System Capacity	passed/failed
IPC queue	passed/failed	
vs (voice system)	The voice system	up/down
Number of Purchased Voice Ports	number of ports	The number of ports on the messaging system that are available for use.
Number of Voice Ports In Service	number of ports	The number of ports that are actually accepting and processing calls on the messaging system. It is recommended that this number matches the number of purchased ports. If it does not, follow the procedure in the Displaying Voice Equipment Status section in the *Communication Manager Messaging Alarms and Events Guide* to identify which ports are not in service.
Available Hours of Speech	number of hours	The number of hours of speech on the messaging system's hard disk that are available for use.
Used Hours of Speech	number of hours	The number of hours of speech that are currently used to store voice messages and other types of messaging data. This number needs to be less than 80 percent of the purchased hours of speech. If the value listed in the report is greater than 80 percent of the purchased hours of speech, contact your sales representative to purchase additional hours of speech.
Maximum Hours of Speech	number of hours	The number of hours of speech left on the hard disk that can be purchased and activated. If this number is 0 and additional hours of speech are needed.
Number of Available Text-to-Speech Sessions	number of sessions	The number of available text-to-speech sessions.

Voice Ports and Speech Storage Status

The voice system (vs) module summarizes voice port and speech storage information.

Viewing system evaluation summary

About this task

You can view the system summary on the System Evaluation page which lists the following :

- Software Summary
- Messaging Announcement Sets
- Switch Integration
- Feature options
- Messaging System Usage Report
- File System Usage Report
- Auto Attendants Report

To view report after evaluating the system:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **System Evaluation**.

Result

The system takes a few minutes to check the hardware installed on the system and generates a summary report of the messaging system.

Accessing the Messaging System Software Display

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Software Management** section, click **List Messaging Software**.

Result

The system takes a few minutes to check the software installed on the system and displays the results on the High Level Packages Installed in Package Priority order page.

Verifying Custom Features

About this task

The messaging system has a variety of customer features. You can verify that an optional feature is enabled for your system by checking its status on the Messaging Custom Features page.

Procedure

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

Viewing the alarm summary

About this task

The Alarm Summary page shows the current status of certain maintenance and security aspects of the system.

The following fields are displayed:

- System Name
- System Time

- Web Server Status
- Message Server Status
- Number of Major Alarms
- Number of Minor Alarms
- Number of Warning Alarms
- Number of entries in the Administrator's Log

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Information** section, click **Alarm Summary**.

Related links

Alarm Summary field descriptions on page 86

Alarm Summary field descriptions

Name	Description
System Name	The name of the Communication Manager server on which the messaging system resides
System Time	The Linux system date and time for which the system monitor is currently showing data.
Web Server Status	Active or inactive. This is the status of the messaging connection to its web server.
Message Server Status	May show messaging in service or messaging out of service.
Number of Major Alarms	The number of major alarms that are current and not yet resolved.
Number of Minor Alarms	The number of minor alarms that are current and not yet resolved.
Number of Entries in the Administrator's Log	The total entries currently in the Administrator's Log. The log allows up to 2000 entries.

Related links

Viewing the alarm summary on page 85

Monitoring Voice Channels in real time

About this task

The messaging system automatically updates the status information provided by the Voice Channel Monitor report. The default setting for the refresh rate is 5 seconds. You can adjust this interval from 1 to 30 seconds while viewing the Voice Channel Monitor.

To display the Voice Channel Monitor:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Information** section, click **Voice Channel Monitor**.
4. In the **Refresh Rate** field, type the new update interval.

   The interval can be any interval between 1 and 30 seconds.
5. Click **Display**.

   The Voice Channel Monitor Display page is displayed.

   Note:

   Shortening the refresh rate consumes more system resources and could adversely affect system performance. Monitor your system after changing this interval to ensure that the system is performing well.

Related links

Voice Channel Monitor Display field descriptions on page 87

Voice Channel Monitor Display field descriptions

Name	Description
Channel	The channel numbers, 0 through 7. Channels are numbered sequentially beginning with the first voice port.
Calls Today	The number of calls made to the channel so far today. Calls are monitored for a 24-hour period beginning at midnight. At midnight, the Channel Monitor is cleared and begins compiling this statistic anew.
Voice Service	When the channel is being used, its service assignment shows up in this column. For example, if a channel is assigned to the messaging service, messaging displays in this column when that channel answers a call.
Service Status	The current status of the channel. The possible status values follow. An asterisk indicates an inactive state; that is, the channel is not processing any calls. • *Broken The channel is broken. Diagnostics did not pass on the card, and it may have to be replaced • CCA The channel is classifying a call; that is, it is monitoring the network for progress tones that indicate, for example, busy or ringing. • Coding The channel is encoding a voice message. • Collect The channel is collecting caller input in the form of touchtones.

Table continues…

Name	Description
	• *Diagnose The channel is undergoing diagnostics by the system software. No incoming calls are being accepted on this channel. • Dialing The channel is dialing digits. This usually means that the channel is currently originating or transferring a call or updating message-waiting indicators. • DIPx A Data Interface Process (DIP) is processing a request from the service on the channel. The quantity of DIPs in progress for different software processes is indicated by the number x. • *foos The channel is in a facility-out-of-service state. The cable coming into the voice card could be unplugged, or the switch may not be configured correctly. • *Initing The channel is being initialized at system start (boot, reboot, or stopping and starting the voice system). • Offhook The channel answered an incoming call or is making an outgoing call. • On Hook The channel is waiting for a call to come in. • *manoos The channel is in a manually-out-of-service state. It was taken off hook intentionally through administration. Incoming calls to this channel receive a busy signal. • *Nonex The channel no longer exists; the card was removed. • *Pending This is a transitory state. Ownership of the channel is being transferred from TSM (for example, the channel is answering calls) to maintenance (for example, the channel is being diagnosed) or vice versa. • Talking The channel is playing a voice message. • Transfer The channel is transferring a call. • *Unknown The channel is experiencing a breakdown in communication.
Caller Input	The last set of touchtones entered by the caller. **Note:** This field does not show subscribers' Voice Messaging passwords. Password keystrokes appear as Xs.
Dialed Digits	The last set of digits dialed by the channel during a transfer attempt.

Related links

[Monitoring Voice Channels in real time](#) on page 86

Verifying Text-to-Speech

Text-to-Speech (TTS) conversion is an optional feature that enables users who access their messaging mailboxes with the telephone to listen to a voiced rendering of email messages.

Accessing Text to Speech parameters

About this task

The Text to Speech (TTS) session default is headers_and_bodies.

The entire text component of the message is voiced.

If a file attachment is included in a message, that component is not voiced. The subscriber hears only summary information about the size of the attached file.

Procedure

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

   The system displays the Administer System Attributes and Features page.
4. In the **Text to Speech Conversion** field, click **Headers and Bodies**.

   The **Headers and Bodies** text to speech option is used to speak text items within message headers as well as the text component of the message body.
5. Click **Save**.

Calling Party Number

Depending on the switch configuration, you can hear up to 39 digits when you hear the message header from a Telephone User Interface or when you retrieve call answer messages using IMAP4 or POP3 clients.

A system administrator can activate the Calling Party Number feature from the **System Administrator** web page (**Messaging Administration** > **System Administration**).

Setting privacy enforcement level for Standards based (IMAP4 and POP3) clients

About this task

A message that is marked private will not be forwarded by the recipient from the Telephone User Interface (TUI).

You can set the privacy enforcement type field to:

- Email: request receiver to keep message private
- Voice mail: enforce privacy

This field only affects the Internet Messaging interface. Therefore, private messages cannot be forwarded from the TUI.

If you set the privacy enforcement type feature to voice mail:

- When you try to send a private message out of the system through SMTP, the message is blocked.
- When an unapproved client tries to retrieve a private message through POP3 or IMAP4, the client gets a correct header, but a localized canned body. The localized canned message indicates that the message is private and cannot be retrieved by the client that is currently being used.

Depending on the privacy enforcement level set, the system blocks a private message to a user and displays a warning message when retrieving the message from IMAP4 or POP3.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **System Administration**.
4. Locate the **Feature Activation** section, and in the **Privacy Enforcement Level** field, select one of the following options:
   - **Voice**: If Voice id messages must be delivered or made available to clients that are known to respect voice-mail style privacy.

     If you select the Voice enforcement type, message forwarding is not available through the TUI or (deprecated) Message Manager.

     The default enforcement level is Voice.

     Note:

     Most email clients (for example: IMAP4, POP3) do not restrict the forwarding of messages.
   - **Email**: If the message must be marked as private and the recipient is requested to keep the message private.

Administering External SMTP Host

About this task

The system forwards the emails that are not addressed to a locally known digitally networked system that supports Internet Messaging to the SMTP relay host.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **External Hosts**.

4. Select the external host that you want to change, and click **Change**.

   If external hosts are not configured for the messaging server, the **Change** and **Delete** buttons are unavailable. You can add a new external host by using the **Add** button.

5. Type the IP address, Host Name and Alias of the external SMTP Server.
6. Click **Save**.

Subscriber Administration

The subscriber administration procedures assume that you know basic messaging commands and navigation, such as logging in to and out of the system.

The following topics provide information on administering the Communication Manager Messaging system and application features that are available to subscribers.

Listing Class of Service Names

About this task

A Class of Service (COS) is a set of messaging capabilities that you define and assign to subscribers. Your system offers 12 classes of service with the default names class0 through class11.

These 12 classes of service, which contain the same default values at installation, are available for you to modify and rename as needed to meet the requirements of subscribers within your organization.

You can assign the same Class of Service to any and all subscribers or assign different classes of service for up to 12 unique groups of subscribers.

The Class of Service screen lists the current name and number for each of the 12 Classes of Service. You can only view the COS names or numbers on this screen; you cannot use this screen to change COS names or numbers. To change COS values, see Changing Class of Service Options on page 92.

To display a list of the current Classes of Service:

Procedure

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

   The system displays the Manage Classes-of-Service page.

Result

You can view the list of the current class of service.

Changing Class of Service options

When you change a Class of Service, that change affects all subscribers to whom you have assigned that Class of Service. For example, if you change the Incoming Mailbox Order field from fifo to lifo for the Class of Service named class8, the order of messages in the incoming mailbox changes for all subscribers with class8 identified on their Subscriber screen.

Making Changes to a Class of Service

About this task

Follow the below procedure to change the attributes of a class-of-service:

Procedure

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

   The system shows the Manage Classes-of-Service page.
4. Select the COS you want to edit and click **Edit the Selected COS**.

   The system shows the Edit a Class-of-Service page.
5. Type appropriate values for the fields and click **Save** .

Edit a Class-of-Service field descriptions

Field	Description
Class of Service Number	The number representing the Class of Service
Class of Service Name	The name of the Class of Service

Table 4: PARAMETERS

Field	Description
Addressing Format	The addressing format. The options are Extension, and Name.
Login Announcement Set	The set used for the login announcement.
System Multilingual is	The multilingual status of the system.
Call Answer Primary Annc. Set	The set used for the primary announcement.
Call Answer Language Choice	The status of the call answer language choice.
Call Answer Secondary Annc. Set	The set used for the secondary announcement.

Table 5: PERMISSIONS

Field	Description
Type	The type of the permission.
Announcement Control	The status of announcement control.
Outcalling	The status of outcalling permission.
Priority Messages	The status of priority messages.
Broadcast	The broadcast permissions.
MCAPI Access	The status of MCAPI access permissions.
MCAPI Message Transfer	The status of MCAPI Message Transfer permissions.
Fax Creation	The status of fax creation permissions.
Trusted Server Access	The status of trusted server access permissions.
Mail User Agent Access	The status of mail user agent access permissions.

Table 6: INCOMING MAILBOX

Name	Description
Order	The order of incoming emails. The options are:LIFO, FIFO
Category Order	The order of the categories of the emails.
Retention Time, New	The new retention time for an email.
Retention Time, Old	The old retention time for an email.
Retention Time, Unopened	The retention time for an unopened email.

Table 7: OUTGOING MAILBOX

Name	Description
Order	The order of outgoing emails. The options are:LIFO, FIFO
Category Order	The order of the categories of the emails.
Retention Time, File	The retention time for a file.
Delivered/Nondeliverable	The status of an outgoing email.

Table 8: MISCELLANEOUS

Name	Description
Voice Mail Message (seconds) , Maximum Length	The maximum character length for the voice mail message.
Minimum needed	The minimum character length required for the voice mail message.
Call Answer Message (seconds) , Maximum Length	The maximum character length for the call answer message.

Table continues…

Name	Description
Minimum needed	The minimum character length required for the call answer message.
End of Message Warning Time (seconds)	The end of message warning time in terms of seconds.
Maximum Mailing Lists	The maximum number of mailing lists.
Total Entries in all Lists	The total number of entries in all lists.
Mailbox Size (seconds), Maximum	The maximum mailbox size in seconds.
Minimum Guarantee	The minimum guarantee.

Table 9: Buttons

Button	Action
Back	Opens the previous page that you visited.
Save	Saves the changes that you made.

Adding Subscribers

About this task

Additional to the initial group of subscribers, you can also add subscribers as new employees join your company.

Note:

When adding a subscriber you can make it an automated attendant, which is described in Automated Attendant and Bulletin Boards on page 170.

Follow the below procedure to add a new subscriber:

Procedure

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

   The system displays the Manage Subscribers page.
4. In the **Local Subscriber Mailbox Number** field, type a new extension and click **Add or Edit**.

   The system displays the Add Local Subscriber page.
5. Type appropriate values for the fields and click **Save**.

   Note:

   The default values for the fields for the Custom COS Sections (optional) group in the Add Local Subscriber page depend on the COS that is assigned to this subscriber. The

initial default values that are specified for some of the fields can change if the COS is changed.

Note:

If you change the contents of any field on the Custom COS sections on the Add Local Subscriber page, the subscriber loses the current Class of Service affiliation. Make changes to this page only if you want a subscriber to have a custom Class of Service.

6. Notify the subscriber that the messaging service is available and provide the subscriber the default password, you have assigned.

Next steps

To complete the task of adding a subscriber, either you or the subscriber must record the subscriber's name.

Otherwise, a caller or voice mail recipient hears the extension number, not the name, of the subscriber. See Creating or Changing Subscriber Name Recordings on page 103 for more information.

If you enter a large number of subscribers, you might want to back up system data. Your exposure to data loss is not very great because if you schedule a nightly backup, the system data file system is backed up automatically every night.

If you need help in backing up system data, see the Data Management chapter.

Add Local Subscriber field descriptions

Name	Valid Input	Description/Procedure
Last Name	A unique name that consists of alphanumeric characters excluding the following symbols: ` | < > ; ^ \	Enter the last name of the subscriber. This is a mandatory input field; there is no default value. The name must be unique. The system combines the last name with the first name to generate the subscriber's name. Subscriber names can contain 1 to 27 characters. Furthermore, in places where telephones have letters that accompany the numbers, each name must be unique as entered on the keypad of a touchtone telephone, for example, Doe,JaneA and Doe,JaneZ to distinguish between two possible Jane Does.
First Name	A unique name that consists of alphabetic characters	Enter the given name of the subscriber.

Table continues…

Name	Valid Input	Description/Procedure
Mailbox Number	A 3-digit to 50-digit telephone extension	Enter the subscriber's mailbox number. The mailbox number must be: • Within the range of numbers assigned to your system. • Not be assigned to another local subscriber. • Of valid length on the local Communication Manager Messaging system. See Changing Local Machine Information on page 122 in the Digital Networking section for more information.
Password	• A number of up to 15–digits in length • Default=Blank	Enter the default password the subscriber must use to log in to his or her messaging mailbox. If you do not enter a password or if you enter a password that is shorter than the Minimum Password Length specified on the Administer System Attributes and Features screen, the subscriber is then required to change the password on the first login.
Class of Service	• A unique name that consists of alphanumeric characters • Default=Class00	Select the name or number of the Class of Service to be assigned to this subscriber. You can change the name of the COS to be more descriptive and convenient for you. See Changing Class of Service Options on page 92. Enter the command **`list cos`** for a list of all current COS names and numbers. See Listing Class of Service Names on page 91 for more information.
Covering Extension:	• Blank • 3 to 10 digits	The number of the default destination for the Transfer Out of Messaging feature. If this field is left blank, the system default covering extension specified on the Administer System Attributes and Features is used. The extension that is entered must be of the correct extension length for the switch.

Table continues…

Name	Valid Input	Description/Procedure
		Security alert: The number you enter in this field must be an administered extension on the switch to minimize the possibility of toll fraud.
MWI Enabled	• yes • no	Set this field to **No** if: • Message waiting indicators must not be sent for this subscriber. Subscriber does not have a phone or switch in the network.
Account Code	0 to 9 digits	This field is used to create call detail records on the switch. See Account Code Billing on page 166 for more information.
Community ID	• A number from 1 to 15 • Default=Blank	Enter the community ID to be assigned to this subscriber. If this field is left blank, the system default community ID from the Machine screen for the local machine is used. See Setting Up Community Sending Restrictions on page 72 for restrictions on sending messages between communities.
Broadcast Mailbox	• y = yes • n = no	When adding a subscriber, this field always displays an n. See Setting Up a Broadcast Mailbox on page 75 for more information on this field.
Secondary Ext	• 3–10 digits, depending on the length of the mailbox • blank	You have the option to enable FAX Messaging with Communication Manager Messaging. You can provide a second extension number for the subscriber for fax reception in this field.
Time Zone	Valid time zone for the subscriber	Messages sent out from a subsciber's mail box is stamped with the administered time zone.
Locked?	• y = yes • n = no	Press the `Tab` key to skip this field. When adding a subscriber, this field always displays an **n**. See Unlocking a Subscriber's Mailbox on page 105 for more information about this field.

Table continues…

Name	Valid Input	Description/Procedure
Messaging Locale	• Default=English	Select the locale setting that must be used for text-based messages to the subscriber.
Email	Email handle and the domain name must not exceed 128 characters.	Enter the subscriber's email handle from Internet Messaging.
Ascii Name	Up to 27 alphabetic characters	Enter the name of the subscriber.
Miscellaneous 1 Miscellaneous 2 Miscellaneous 3 Miscellaneous 4	1 to 11 alphanumeric characters	Enter additional information about the subscriber that could be helpful to you. Any entry in this field is for your convenience only and is not used by the messaging system.
Time Zone	Select a unique time zone for a subscriber	

The rest of the section refers to Custom Class Of Service. The fields in these sections are explained in Edit a Class-of-Service page on page 92.

Changing Subscriber Data

About this task

After the initial group of subscribers has been added, you can change subscribers as existing employees require expanded messaging services.

Note:

Use the Manage Subscriber page to add or edit local subscribers and add remote subscribers. Automated Attendant is described in Automated Attendant and Bulletin Boards on page 170.

You can change a subscriber's name or mailbox number without disrupting mailing lists because a unique, system-generated subscriber ID, not the name or mailbox number, actually links the subscriber's mailbox to lists and personal directories. The system-generated ID is not accessible to you. Lists are automatically updated with name changes. For example, if Jane Doe is on a mailing list and her name is changed to Jane Smith, the list is updated automatically to reflect the change.

If you change a subscriber's name, you or the subscriber must record a new name fragment over the subscriber's existing name fragment to reflect this change. See Creating or Changing Subscriber Name Recordings on page 103 for more information.

To change subscriber data:

Procedure

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

   The system displays the Manage Subscribers page.

4. Perform one of following actions:
   - In the **Local Subscriber Mailbox Number** field, type the mailbox number of the local subscriber and click **Add or Edit**.
   - Click **Manage**, for either **Local Subscribers** or **Remote Subscribers**.
5. Change subscriber information.
6. Click **Save**.

Removing Subscribers

About this task

After the initial group of subscribers has been added, you can delete subscribers as employees leave your company.

Removing a subscriber means deleting the subscriber's name and mailbox number from the system directories and deleting the subscriber's recorded name fragment. You need to remove subscribers any time they leave your company or no longer require the messaging service.

After the subscriber is removed, all records pertaining to the subscriber are deleted automatically by messaging audits that are executed every Sunday morning at 1:00 a.m. For more information about audits, see Voice Messaging Database Audit Overview on page 198.

To remove a subscriber:

Procedure

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

   The system displays the Manage Subscribers page.
4. Click **Manage**, for either **Local Subscribers** or **Remote Subscribers**.
5. On the Manage Local Subscribers page, select a subscriber from the list.
6. Click **Delete the Selected Subscriber**.

   The system displays a pop-up window with the message:

   ```
   Are you sure that you want to remove this subscriber?
   ```
7. In the messaging pop-up window, click **OK**.

Result

The selected subscriber in now deleted from the list.

Listing Subscribers

Listing Subscribers by Name

About this task

You can sort and filter the subscribers list by their names. The names of local subscribers are listed along with their mailbox numbers, classes of service, and Community ID.

To list administered messaging subscribers:

Procedure

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

   The system displays the Manage Subscribers page.
4. On the Manage Subscribers page, perform one of the following action:
   - In the **Local Subscribers** row, click **Filter** to view the Sort and Filter Local Subscribers page.
   - In the **Local Subscribers** row, click **Manage** > **Sort and Filter** to view the Sort and Filter Local Subscribers page.

   You can perform the same steps, for the **Remote Subscribers** also.

   The system displays the Sort and Filter Local Subscribers page.
5. In the **Name** row, click on **Primary**.

   The Primary column determines the first sort key in ascending or descending order.
6. Perform the following actions in the **Name** row:
   a. In the **Form** field, type the starting name of a subscriber list, that you want to sort.
   b. In the **To** field, type the end name of that subscriber list.
7. Click Save.

Result

The system displays the changed sort order in the subscriber list.

Listing Subscribers by Mailbox Number

About this task

You can sort and filter the subscriber list by their Mailbox Number. This feature is applicable for remote subscribers also.

To list administered messaging subscribers:

Procedure

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

   The system displays the Manage Subscribers page.
4. On the Manage Subscribers page, perform one of the following action:
   - In the **Local Subscribers** row, click **Filter**, to view the Sort and Filter Local Subscribers page.
   - In the **Local Subscribers** row, click **Manage** > **Sort and Filter**, to view the Sort and Filter Local Subscribers page.

   You can perform the same steps for the **Remote Subscribers** also.

   The system displays the Sort and Filter Local Subscribers page.
5. In the **Mailbox Number** row, click on **Primary**.

   The Primary column determines the first sort key in ascending or descending order.
6. In the **Mailbox Number** row, perform the following actions:
   a. In the **Form** field, type the beginning of a mailbox number of the included range.
   b. In the **To** field, type the end of a mailbox number of the included range.
7. Click **Save**.

Result

The system displays the changed sort order in the subscriber list.

Listing Subscribers by Class Of Service

About this task

Sort and filter the subscribers list by the class-of-service of each local subscriber. This feature is not available for remote subscribers.

Procedure

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

   The system displays the Manage Subscribers page.

4. On the Manage Subscribers page, perform one of the following action:
   - In the **Local Subscribers** row, click **Filter**, to view the Sort and Filter Local Subscribers page.
   - In the **Local Subscribers** row, click **Manage** > **Sort and Filter**, to view the Sort and Filter Local Subscribers page.

   You can perform the same steps for the **Remote Subscribers** also.

   The system displays the Sort and Filter Local Subscribers page.
5. In the **Class Of Service** row, click on **Primary**.

   The Primary column determines the first sort key in ascending or descending order.
6. In the **Class Of Service** row, perform the following actions:
   a. In the **Form** field, select the starting class of service from the drop-down list of the included range.
   b. In the **To** field, select the ending class of service from the drop-down list of the included range.
7. Click **Save**.

Result

The system displays the changed sort order in the subscriber list.

Listing Subscribers by Community ID

About this task

Sort and filter the subscribers list by the community to which each one is assigned. This feature is available for remote subscribers also.

To sort and filter subscriber by their community IDs:

Procedure

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

   The system displays the Manage Subscribers page.
4. On the Manage Subscribers page, perform one of the following action:
   - In the **Local Subscribers** row, click **Filter** to view the Sort and Filter Local Subscribers page.
   - In the **Local Subscribers** row, click **Manage** > **Sort and Filter** to view the Sort and Filter Local Subscribers page.

   You can perform the same steps for the **Remote Subscribers** also.

   The system displays the Sort and Filter Local Subscribers page.

5. In the **Community ID** row, click on **Primary**.

   The Primary column determines the first sort key in ascending or descending order.

6. In the **Community ID** row, perform the following actions:
   a. In the **Form** field, select the starting community id from the drop down list of the included range.
   b. In the **To** field, select the ending community id from the drop down list of the included range.
7. Click Save.

   The system displays the changed sort order in the subscriber list.

Listing remote email users

About this task

The system saves address and delivery information for emails delivered outside of the messaging domain.

Procedure

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

   The system displays the Remote Text Addresses page.
4. Select the machine you want to view the remote text addresses.
5. Click **List Addresses**.

Result

The system displays the list of the remote text addresses.

Creating or changing Subscriber Name Recordings

About this task

The subscriber name recording is the spoken name that is recorded for or by each messaging subscriber. This fragment is spoken by the messaging system during call answering, such as "Your call is being answered. Jane Doe is not available." The first fragment ("Your call is being answered.") and the third fragment ("is not available.") are messaging system fragments. The second fragment ("Jane Doe") is the subscriber's recorded name fragment. If a name is not recorded, callers or message recipients hear the mailbox number, not the name, of the subscriber.

You have two options for recording subscriber names:

- Record the names yourself from the extension that has announcement control permission.
- Activate the Name Record by Subscriber feature on the Administer System Attributes and Features screen. Then, the messaging system asks each subscriber to record a name the first time that she or he logs in. If you record subscribers' names before they log in for the first time,

they are not prompted to record their names. However, subscribers always have the option of recording their names by using the telephone.

To create or change a subscriber's name recording:

Procedure

1. From your telephone, dial the messaging system extension.
2. Enter your extension (the one that has announcement control permission) followed by the pound sign (#) when prompted.
3. Enter your password followed by the pound sign (#) when prompted.
4. Press 9 to perform system administration.
5. Press 4 to record a subscriber's name.
6. Enter the mailbox number of the subscriber whose name you are about to record followed by the pound sign (#) when prompted.
7. Speak the subscriber's name clearly when prompted.
8. Press the pound sign (#) to signify the end of the recording.
9. When you are finished with this subscriber name recording, choose one of the following:
   - Repeat Step 6 to Step 8 for each additional subscriber name you want to add or change.
   - Press # 7 to return to the Activity menu or just hang up to exit the messaging system.

Enabling subscribers for automatic mail forwarding to SMTP

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Subscriber Management**.
4. In the **Local Subscribers** row, click **Manage**.
5. Select the subscriber that you want to edit, and click **Edit/Delete the Selected Subscriber**.
6. In the **Forwarding Destination Address** field, type the destination email address.

   For example, type johns@gmail.com.

   Do not select the **Delete after Forward?** check box if you want to retain the original copy of the message in the inbox.

Resetting subscriber passwords

About this task

If a subscriber forgets his or her password, you must reassign, through the Subscriber screen, a new password to allow the subscriber to again log in to the messaging system. The subscriber should then change the password to a unique, subscriber password.

Procedure

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

   System displays the Manage Subscribers page.
4. Click **Manage** for Local Subscribers or Remote Subscriber depending on the type of subscriber whose extension you want to change.

   The Manage Local Subscribers or Manager Remote Subscribers page is displayed
5. Select the subscriber from the list.
6. Perform one of the following action:
   - Click **Edit/Delete the Selected Subscriber** for local subscribers.
   - Click **Edit the Selected Subscriber** for remote subscribers.
7. Under the **Basic Information** group, in the **Password** field, type a new password.

   See Changing Subscriber Data on page 98 for more information.
8. It is recommended to enter a shorter password than the required length, so that the subscriber must change the subscriber password on the next login.

   The system places some constraints on passwords to improve security.

   A subscriber password cannot:
   - Be the same number as the mailbox number (forward or reverse).
   - Be a subset of the subscriber password (forward or reverse), if the password is more than three digits long.
   - Be a subset of the mailbox number (forward or reverse).
   - Be all of the same digit (if more than one digit is entered). For example, 1111 is not allowed.
   - Be a string of consecutive numbers. For example, 12345 or 7654 are not allowed.
9. Click **Save** to save the changes in the system database.

Unlocking a Subscriber's Mailbox

Things to Consider About Unlocking a Subscriber's Mailbox

Security/toll fraud	If a subscriber is repeatedly locked out of the messaging system, some unauthorized person may be attempting to tamper with that subscriber's mailbox. Report this to the subscriber's manager or

	to your company security office before unlocking the login ID. If the unsuccessful login attempts were made from an extension other than that of the owner of the mailbox, the Administrator's Log contains information about the break-in attempts.

Unlocking a Mailbox

About this task

A subscriber mailbox can become locked after too many unsuccessful login attempts. Follow the below procedure to unlock a subscriber mailbox:

Procedure

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

   System displays the Manage Subscribers page.
4. Click **Manage** for Local Subscribers or Remote Subscriber depending on the type of subscriber whose extension you want to change.

   The Manage Local Subscribers or Manager Remote Subscribers page is displayed
5. Select the subscriber from the list.
6. Perform one of the following action:
   - Click **Edit/Delete the Selected Subscriber** for local subscribers.
   - Click **Edit the Selected Subscriber** for remote subscribers.
7. Under the **Basic Information** group, verify that the **Locked** field is set to **yes**.
8. Select **no** from the drop-down list to unlock the mailbox.
9. Click **Save**.

Result

For security purposes, the messaging system allows only three login retries per user session before disconnecting. The messaging system also monitors the number of unsuccessful consecutive login attempts to a specific mailbox across multiple calls to the messaging system.

If this number exceeds the number defined in the **Login Parameters** section of the Administer System Attributes and Features page, the messaging system locks out that subscriber login ID, thus preventing further system access. The subscriber cannot access the messaging system until you unlock the subscriber login.

Messaging system administration

Accessing the Product ID

About this task

The product ID identifies the Communication Manager. You must have the product ID when you are contacting your remote maintenance service center.

To access the product ID:

Procedure

1. At the Linux prompt, type `productid` and press `Enter`.

   The system displays a list of installed products.

2. Verify that the system displays the server product ID, messaging product ID, and the RMB product IDs.

   Note:

   If the IDs are not displayed, you must reinstall the system.

Starting the Messaging software (Voice System)

Procedure

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

   The system displays data indicating processes are starting. The system displays the following message when the startup is complete:

   ```
   Startup of the Voice System is complete.
   ```

   If the voice messaging system has been stopped in order to Administer Switch link, you can restart the voice messaging system by clicking Start Messaging link on the left hand panel.

Restarting the Messaging System

Procedure

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

   The system displays the Stop Messaging Software page.

4. Click **Stop**.

The Stop Messaging Software Web page refreshes periodically during the shutdown process and displays a status message following the **Stop Messaging info** text.

After the Messaging software stops completely, the system displays the `Stop of Messaging completed` message.

5. Click **OK**.
6. In the left hand pane, under the **Utilities** group, click **Start Messaging**.

   The system displays the Start Messaging Software page.

   The Start Messaging Software Web page refreshes periodically during the startup process and displays a status message following the **Start Messaging information** text.

   After the Messaging software starts successfully, the system displays the `Start of Messaging completed` message.

Stopping the Messaging Software (Voice System)

About this task

Note:

Stop the voice system only when it is absolutely necessary. When the voice system is stopped, callers to messaging hear a fast busy signal, and callers who are sent to messaging coverage hear ringing with no answer.

Procedure

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

   The system displays a pop-up window with the message:

   `Stop of Messaging completed.`

   The SMI web page displays the following message:

   `Messaging stop is complete at <date/time>.`
5. In the messaging pop-up window, click **OK**.

   Note:

   To view messaging administration web pages, you must restart the voice system.

Shutting down the system

Before you begin

You must stop messaging before shutting down the server.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the Administration menu, click **Server (Maintenance)**.
3. In the **Server** section, click **Shutdown Server**.

   The system displays the Shutdown This Server screen.
4. Do one of the following: Click the **Delayed Shutdown** radio button to wait for messaging subscribers to logoff or **Immediate** to shutdown immediately.
   - To wait for messaging subscribers to logoff, click **Delayed Shutdown**.
   - To stop messaging immediately, click **Immediate**.

   If you do not stop messaging and select Immediate shutdown, the messaging databases might become corrupt and you might lose data.

   Leave the **Restart system after shutdown** option blank.
5. Click **Shutdown**.

   The system responds by shutting down the system.

Checking the Restart Causes

About this task

The Communication Manager server system keeps track of the system restarts. Use this log to determine when to perform the next restart.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. Log in with super user credentials.
3. On the **Administration** menu click **Server (Maintenance)**.
4. In the **Diagnostics** section, click **System Logs**.
5. In the **Select Log Types** section, select the **Linux login/logout/reboot log** check box.
6. In the **Select Event Range** section, select the dates for which you want to view system logs.
7. Click **View Log**.

   The system displays the View System Logs page.
8. Check the information on the screen for the best date to reboot the system.
9. To reboot the system, continue with Performing a System Restart on page 110.

Performing a System Restart

About this task

Note:

You cannot restart your system if a backup is running.

To perform a restart:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the **Server** section, click **Shutdown Server**.

   The system displays the .
4. On the Shutdown Server page, do one of the following:
   - Click the **Delayed Shutdown** option to wait for messaging subscribers to logoff.
   - Click **Immediate** to shut down immediately.
5. Ensure that the **Restart server after shutdown** option is selected.
6. Click **Shutdown**.

   The system responds by shutting down the system and then restarts.

Enhanced-List application administration

The Enhanced-List Application (ELA) greatly expands the ability to deliver messages to large numbers of recipients.

Note:

In addition to or instead of ELA mailing lists, subscribers can access email mailing lists by setting up a list on an email list server and then addressing messages to the list. The system administrator must add a remote subscriber corresponding to the list, as described in Adding a Remote User manually on page 143, and will need to add the list server as a Communication Manager Messaging trusted server.

Planning for Enhanced List Application Implementation

What you need before you begin

Before you begin implementing ELA on the system, you must have the following information:

- An available Class of Service (COS) number. This COS number is used by ELA for list mailboxes and the shadow mailbox. If possible, you must use COS 8.

- A community ID for the shadow mailbox. Ideally, the shadow mailbox, as well as the shadow mailboxes of other networked machines, is the only occupant of the selected community. If possible, use community 11.
- A community ID for the ELA list mailboxes. All the list mailboxes must reside in the same community. This community cannot be the same number as the shadow mailbox community. If possible, use community 10.
- A range of extensions to use for list mailboxes. You do not need this to set up ELA but you must provide extensions for the list mailboxes when you begin creating lists.

Scheduling ELA message delivery

You must schedule delivery for large enhanced lists during off-peak hours. This is because during peak traffic hours, your system processes other subscriber-generated messages. ELA intentionally slows delivery of messages to large enhanced lists during peak traffic so your system can continue to process other messages.

Local area networks

If your configuration includes a local area network, involve your LAN administrators in the ELA implementation to ensure that the system and the network are not adversely affected. The amount of traffic on your LAN from ELA messages could increase if ELA sends messages for delivery to email or to TCP/IP-networked remote machines. If none of these are valid for your site, ELA will not cause any increase in LAN traffic.

Remote messages

If your site is networked, estimate the increase in the amount of remote traffic by determining the percentage of current traffic that is remote and by calculating the number of messages per minute that percentage represents. When ELA is actively sending messages, add that number of messages to the traffic estimate for remote message delivery.

Call answer messages

ELA lists can also be used to distribute call answer messages. So, anyone can call the ELA list mailbox and leave a message. The system then distributes this message to all subscribers in the list. To receive a call answer message, you must administer the ELA mailbox number as an extension on the switch and set the call coverage path to the message server hunt group.

Nested lists

One ELA list can contain another ELA list. For example, you can create ELAlist1 and make ELAlist2 as one of its members. This nesting will automatically include the members of ELAlist2 in ELAlist1. Including a nested list in this example results in only one member (ELAlist2) counting against the ELA list member limit of 1500.

Note:

A nested ELA list cannot include the ELA list in which it is nested. For example, if ELAlist2 is nested inside ELAlist1, then ELAlist2 cannot include ELAlist1. The system displays an error if you try to nest a list in this way. However, if you include a non-ELA list within an ELA list, the system cannot check that the non-ELA list also includes the ELA list. If you include a non-ELA list within an ELA list, the system may get into an infinite loop of sending messages, which might cause your subscribers to receive multiple messages.

Shadow mailbox

The shadow mailbox is a special mailbox that ELA uses to distribute messages. You can administer enhanced lists through the **Permit Reply** field on the Create a New Enhanced-List page so that recipients can reply to:

- The person who originally sent the message.
- All recipients of the original message.

You can also administer the **Permit Reply** field so that recipients cannot reply. A properly-configured ELA shadow mailbox helps the system block recipients from replying to ELA senders or recipient lists. The shadow mailbox must belong to a community that cannot receive messages, but can send messages to all other communities.

Administering the messaging system for ELA

Procedure

1. Define an ELA Class of Service.
2. Set up the ELA and shadow mailbox Community IDs.
3. Create a system shadow mailbox.
4. Create a system broadcast mailbox, if any ELA lists will be administered as broadcast lists.

Administering ELA for the messaging system

Procedure

1. Configure ELA.
2. Create enhanced lists.
3. Add members to enhanced lists.
4. **(Optional)** Record a name for the enhanced lists.
5. Test the enhanced list setup.

Administering ELA for default Enhanced-List Attributes

About this task

While configuring ELA, you can set the default attributes of the Class-of-Service and Community ID. The default Enhanced-Lists can receive from any community and send messages to any community. This list is different from the Shadow Mailbox, where the shadow mailbox is analogous to a postmaster. Subscribers cannot reply to a shadow mailbox list.

To set up the ELA default community ID, you must administer a CMM Classes-of-Service with the recommended values for ELA.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Classes-of-Service**.

The system displays the Classes-of-Service.

4. Select a Class-of-Service, and click **Edit the Selected COS**.
5. Ensure that the **Addressing Format** field is set to **Extension**.

   Refer Class-of-Service settings on page 113for the settings for the other fields on the Edit a Class-of-Service page.
6. Click **Save**.

Class-of-Service settings

Name	Setting
Addressing Format	Extension
Login Announcement Set	System
Call Answer Primary Annc. Set	System
Call Answer Secondary Annc. Set	System
PERMISSIONS	
Type	call-answer
Announcement Control	no
Outcalling	no
Priority Messages	yes
Broadcast	none
MCAPI Access	no
MCAPI Message Transfer	yes
Fax Creation	yes
Trusted Server Access	yes
INCOMING MAILBOX	
Order	FIFO
Category Order	nuo
Retention Times (days), New	14
Old	14
Unopened	14
OUTGOING MAILBOX	
Order	FIFO
Category Order	unfda
Retention Times (days), File Cab	0
Delivered/Nondeliverable	1
MISCELLANEOUS	
Voice Mail Message (seconds), Maximum Length	1200

Table continues…

Name	Setting
Minimum Needed	32
Call Answer Message (seconds), Maximum Length	1200
Minimum Needed	8
End of Message Warning Time (seconds)	[ ] default
Maximum Mailing Lists	25
Total Entries in All Lists	250
Mailbox Size (seconds), Maximum	8400
Minimum Guarantee	0

Configuring ELA

About this task

ELA configuring can be done for a shadow mailbox or for a default mailing list. Each list serves a specific purpose.

The shadow mailbox list can send messages to any community but cannot receive messages from any community.

The default mailing list can send messages and receive messages from any community.

On the Enhanced-List application page, you can:

Configuring ELA on page 114

Administering ELA for default Enhanced-List Attributes on page 112

To administer the ELA shadow mailbox attributes, you must have an extension for shadow mailbox and a community ID.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Enhanced List Setup**.
4. In the **Mailbox Extension** field, type the extension for the shadow mailbox.

   Note:

   To configure ELA, you must create a shadow mailbox.
5. Decide the community ID that you want to use for the shadow mailbox.
6. In the **Messaging Administration** section, click **Sending Restrictions**.
7. In the Sender Community row, select the **Recipient Community** column corresponding to the community ID.

All check boxes will be selected. No Recipient Community will be able to send messages to the selected sender community.

8. Click **Save**.
9. In the **Messaging Administration** section, click **Enhanced List Setup**.
10. In the **Shadow Mailbox Attributes** section, select the Community ID for which you set restrictions.
11. Click **Save Changes**.

Creating a Shadow Mailbox

About this task

The shadow mailbox is a special mailbox, analogous to a postmaster mailbox, that ELA uses to distribute messages. With a shadow mailbox, replies to ELA-delivered messages are not sent back to the entire enhanced list. However, you can administer enhanced-lists so that recipients can reply to the person who originally sent the message. The shadow mailbox must already exist in the system before you configure ELA.

You can set up one shadow mailbox that serves all enhanced lists on the system.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Local Subscribers** row, click **Manage**.
4. On the Manage Local Subscribers page, click **Add a New Subscriber**.
5. In the **Last Name** field, type a name that is useful to your subscribers, such as Mailing List or Enhanced-Lists Postmaster.
6. In the **Password** field, type any password.

   You cannot leave this field blank.
7. In the **Mailbox Number** field, type an unused mailbox number at which you want the shadow mailbox to be located.

   Make sure that this mailbox number is not administered as a station on the switch.
8. In the **Class of Service** field, click the ELA class-of-service number.
9. In the **Community ID** field, click the number of the shadow mailbox community you created.
10. In the **Email** field, type the same mailbox number followed by the domain name, for instance, 30119@vision-sam1.dr.avaya.com.
11. Leave the default values in all other fields.
12. Click **Save**.

Result

Verify the subscriber is added.

Adding a new Enhanced-List

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Enhanced List Management**.

   The system displays the Manage Enhanced-Lists page.
4. Click **Create a New List**.
5. In the **List Name** field, type a name for the mailing list so that the list can be easily identified as an enhanced-list.
6. In the **Extension** field, type an unused number within your extension range.

   If you use an extension that is in use, the system will convert it to an ELA mailing list
7. In the **Password** field, type a password.
8. In the **Permit Reply to Sender?** field, click **Yes**.
9. In the **Class-of-Service** field, click the Community that you selected on the Configure the Enhanced-List Application page under the **Default Enhanced-List Attributes** section.
10. In the **Community ID (CID)** field, click the ID that you selected for the default Enhanced-List.
11. Click **Save**.

Administering an ELA List

About this task

After you create an Enhanced-List, the list is displayed on the Managed Enhanced-List page.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Enhanced List Management**.

   The system displays the Manage Enhanced-Lists page.
4. View the list of created ELAs on the page.
5. From the list, select an ELA that you want to edit.

   One ELA list can have sub ELA lists within it.

6. You can do the following on the Managed Enhanced-List page:
   - Create a new list. See Adding a new Enhanced-List on page 116
   - Change Attributes of Selected List
   - Sort by names
   - Sort by Extension
   - Open an ELA list - View the existing extensions, add new extensions. You can add local, remote subscribers and email addresses. If you type in a last name that is common to more than one subscriber, the system pops up a window to ask you select the desired subscriber.
   - Display report of all the lists
   - Delete an ELA list
7. Click **Save**.

Administering ELA auto-attendant

About this task

Setting up a subscriber as a auto-attendant and assigning to it an extension of an Enhance-List allows a subscriber to call up this ELA auto-attendant and use the automated attendant menu.

Create an automated attendant menu to serve a specific purpose, for instance, guest-greetings, call-answer to ELA.

To set up the administer an ELA auto-attendant:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Subscriber Management**.
4. In the **Local Subscribers** row, click **Manage**.
5. On the Manage Local Subscribers page, click **Add a New Subscriber**.
6. Enter relevant data to add a new subscriber.
7. In the **Type** field, click **auto-attendant**.
8. In the **Automated Attendant Menu** section, for each button that a caller presses on the touch dial phone, specify how the extension is treated.

   For instance, for Button 1, type an ELA extension with treatment as Call Answer. When a subscriber calls the auto-attendant, the subscriber may listen to a voice recording explaining the functionality of each button on the touch dial phone. When the subscriber presses 1 on the phone, the call is transferred to the ELA extension and the caller can leave a call-answer message for the ELA extension. Subsequently, all the extensions part of that ELA list will receive that call-answer message.

9. Click **Save**.

Testing Enhanced-Lists

About this task

After you configure ELA and create enhanced lists for the system, complete the following steps to test the enhanced lists.

See your installation information if you need help with the following procedures:

Procedure

1. Set up two test subscribers with two test telephones.
2. Create a test list with subscribers test-1 and test-2 as members.
3. Use the test-1 telephone to create and send a voice mail message to the ELA mailbox.

   Record the following or a similar test message and then enter the address for the enhanced-list mailbox:

   ```
   This is a test ELA message for the messaging system.
   ```
4. Hang up the test-1 telephone to disconnect.
5. Verify that the MWIs for the test subscribers' telephones are activated and that the test subscribers received the message.
6. Delete the test messages.
7. **(Optional)** Delete the test subscribers.
8. **(Optional)** Delete the test list.

Administering Call answer disclaimer

About this task

When you enable the Call answer disclaimer feature on a mailbox, the system plays the disclaimer announcement followed by the system or personal greeting. The system plays the disclaimer announcement in the non-dial through mode.

To activate Call Answer Disclaimer on a mailbox, you must activate the feature from the Messaging Custom Features page.

Note:

The system does not play the disclaimer announcement when the mailbox is full. The system also does not play the disclaimer announcement for calls that reach the mailbox through a fax extension.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Classes-of-Service**.

4. Select a Class-of Service, and click **Edit the Selected COS**.
5. In the **Call-Answer Primary Annc. Set** field, click **system**.

   The system uses the setting of the **System Announcement Set** field on the System Administration screen.
6. Set the value of the **Type** field in the **Permissions** section to `disclaimer`.

Enhanced-Lists maintenance

Checking the administrator log

About this task

The system warns you of potential administrative problems with ELA by displaying a minor alarm or warning message (Alarms: w or Alarms: m) when it logs an administration event.

Check for ELA-specific events regularly to monitor ELA performance. To view ELA-specific log entries:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Logs** section, click **Administrator**.
4. Select the starting date and time.
5. In the **Application** field, click **EL**.
6. Click **Display**.
7. Examine the displayed entries.
8. If required, take corrective action.

Checking the delivery failure log

About this task

The delivery failure log contains entries for failed deliveries, a description of the cause of the failure, and other information. Check this log to monitor ELA and system performance and if a subscriber complains that messages are not being delivered.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Logs** section, click **ELA Delivery Failures**.
4. Examine the displayed entries.
5. If required,. take corrective action.

Digital networking administration

This topic provides the information on administering TCP/IP digital networking for Communication Manager Messaging.

The initial administration tasks section provides a list of the tasks you must complete if you are performing initial digital networking administration.

- Initial administration tasks on page 120
- Change the number of administered remote subscribers on page 122
- Administer TCP/IP LAN connectivity on page 122
- Change local machine information on page 122
- Add a remote machine on page 126

  or change remote machine information on page 130
- Renaming a remote machine on page 130
- Record remote machine names on page 131
- Delete remote machines on page 132
- Retrieve a deleted remote machine on page 132
- List address ranges for network machines on page 133
- List remote extensions on page 134
- View a list of machines on page 135
- Display machine information on page 135
- Test the digital networking and TCP/IP connection on page 135

Digital networking initial administration tasks

About this task

The technician performs some of these initial administration tasks at the time of installation. Confirm that each of the tasks was performed. If not, you must complete the task. Ensure that you have the necessary information for TCP/IP, network channels, the local machine, and all remote machines.

Procedure

1. Complete the switch administration on page 13.

   Switch administration is normally done by the technician at the time of installation to define the switch to work with the messaging digital networking ports.

2. Verify or change the number of administered remote subscribers on page 122 to ensure that the number of administered remote subscribers is equal to or greater than the number of all mailboxes on all remote systems.

   The technician changes the number of administered remote subscribers at the time of installation.

3. Administer TCP/IP LAN connectivity on page 122.
4. Change the local machine on page 122 to define local machine information for digital networking.
5. Add a remote machine on page 126 or change a remote machine on page 130.

   Normally, the technician adds or changes the remote machine during installation.

   On the local machine, define the information about each remote machine.
6. Administer the messaging software on the remote machines.

   On each remote machine, define the information about the local machine.
7. Set up remote updates on page 139 to define remote update capabilities for the local machine and remote machines.
8. Perform a full remote update on page 140.

   Manually run a remote update for each remote machine to bring the network up to date immediately.
9. Set automatic deletion on page 142 of non-administered remote subscribers.
10. View remote extensions on page 141 to verify that remote subscribers were added to the local database.
11. Record the names of remote systems so that local subscribers hear voiced confirmations when they are addressing messages to subscribers on those remote systems.
12. Administer remote subscribers on page 143.

    Add, delete, and change subscribers manually when you are not adding all remote subscribers or when non-administered subscribers exist.
13. Record remote subscriber names on page 146 for subscribers not added by a full remote update so that local subscribers hear voiced confirmations when they address messages to remote subscribers.

Display remote machine information

About this task

To display the machine information for a remote machine:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **Networked Servers**.

   The system displays the Manage Networked Servers page. View information about a networked server.

From this page, you can display the machine information for the local machine or any remote machine.

Changing the number of administered remote subscribers

About this task

The number of administered remote subscribers must be equal to or greater than the total number of mailboxes on all remote systems with which the local system networks.

Procedure

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

   The system displays the Limits page .
4. In the **Maximum Administered Remotes** field, type the number of required remote subscribers.
5. Click **Update Limits**.

Administering TCP/IP LAN connectivity

Note:

Avaya is not responsible for the installation, administration, or testing of the LAN. Seek service as directed by your LAN administrator to resolve LAN problems.

Communication Manager and Communication Manager Messaging (CMM) are connected over the LAN using TCP/IP LAN connections. CMM uses these connections for digital networking and (deprecated) Message Manager.

To check these connections, check the IP Interfaces and media gateway screens using the Communication Manager server SAT command line interface.

Changing local machine information

About this task

If you change the local machine profile, contact all remote network administrators and inform them of the changes.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **Messaging Server Admin**.

   The system displays the Edit Messaging Server page.

4. Enter appropriate values in the fields on the Edit Messaging Server page.

   The Voice ID fields are read-only and cannot be changed.

5. Click **Save**.

   See Remote User Administration on page 137 for more information on remote updates.

Edit Messaging Server field description

Field	Valid Input	Description
Server Name	1 to 8 alphanumeric characters A dash ('-') An underbar ('_'). If this is a remote server name, you can enter 1 to 10 alphanumeric characters.	Use this field to enter the unique name of the server you want to add or modify. The server name cannot contain a period, or begin with a digit. Use of the server name "fax" is reserved and not permitted. For the LDAP server type, the server name must be the same as the DNS name.
IP Address	Display-only	The IP address of the local Communication Manager server.
Password	From 5 to 10 alphanumeric characters; can include dashes or underscores	Enter the remote password that machines must use to establish networking connections to this local Communication Manager server.
Server Type	TCPIP	Use the TCPIP server type for Audix digital networking.
Extension Length	As defined on the Switch Link Admin page	Use this drop-down list to select the extension length for all subscribers on this networked server. This number must match the number of digits in the extension numbers defined in the fields under Address Ranges.
Default Community	The default for this field is 1.	Use this drop-down list to select the default community number for this networked server. The community determines the subscriber sending restrictions. The default community is used for messages received from this networked server without the originator's community number.

Table continues…

Field	Valid Input	Description
Voice Name	• YES indicates a voiced name is recorded. • NO indicates a voiced name is not recorded.	This field indicates whether a voiced name for this server is recorded.
Send to Non-Administered Recipients	• If you select Yes, the Messaging system will attempt to deliver messages to non-administered remote recipients. • If you select No, the Messaging system will not attempt to deliver messages to non-administered remote recipients.	Use this drop-down list to enable or disable message delivery to non-administered remote recipients. The system displays this field only when the server tpe is TCPIP.
Voice ID	Internally assigned identifier for the voiced machine name.	The administrator uses this value when recording the name for the machine.
Updates In	yes no	If you select yes, this local Communication Manager server accepts updated subscriber database information from any remote Communication Manager server. The Updates In field must also be set to y on the remote Machine Profile screen setup on the local Communication Manager server for each remote Communication Manager server. If you select no, the local Communication Manager server does not accept updates from any remote Communication Manager server, regardless of the entry on the remote Machine Profile screen. Set this field to yes only after testing the network end to end during initial administration.
Updates Out	yes, no	If you select yes, updates to subscriber database information for local subscribers are sent to a remote Communication Manager server. The Updates Out field must also be set to y on the remote Machine Profile screen set

Table continues…

Field	Valid Input	Description
		up on the local Communication Manager server for each remote Communication Manager server. If you select no, updates are not sent to any remote Communication Manager server, regardless of the entry for this field on the remote Machine Profile screen. Set this field to yes only after testing the network end to end during initial administration.
Remote LDAP Port	For the local server, the default value for this field is the port specified in the LDAP Directory Update Port field on the System Administration page.	Use this field to specify the port used when the system connects to this network device to send directory updates. For a networked server, this field is displayed only if the server type is LDAP.
Inbound LDAP Security	Must use SSL: To use Secure Socket Layer (SSL) encryption for inbound LDAP directory updates Must use SASL or SSL: To use Simple Authentication and Security Layer (SASL) or SSL encryption for inbound LDAP directory updates	Use this field to specify the encryption type required for the connection between the messaging server and a remote networked machine for inbound LDAP directory updates. This field is unavailable if the **Updates In** field is set to `no`. For a networked server, this field is displayed only if the server type is LDAP.
Log Updates In	Yes No	Use this field to enable logging of all incoming updates. Logging incoming directory updates increases the amount of time required to complete a directory update.
Prefix	The prefix can be 0 to 21 alphanumeric characters in length. Total length cannot exceed 24 characters.	Use this field to enter the prefix digits for the ranges of telephone numbers for subscribers on this server. The prefix can be used to distinguish between server that have overlapping extension number ranges.
Starting Mailbox Number	The total length of the prefix and mailbox number cannot exceed 24	Use this field to enter the starting mailbox numbers for the ranges of

Table continues…

Field	Valid Input	Description
	characters, and the ranges cannot overlap with another range if multiple address ranges are specified for this server.	telephone numbers used by subscribers on this server. The number of digits in a mailbox number must match the entry in the Extension Length field for this server.
Ending Mailbox Number	The total length of the prefix and mailbox number cannot exceed 24 characters, and the ranges cannot overlap with another range if multiple address ranges are specified for this server.	The ending mailbox numbers for the ranges of telephone numbers used by subscribers on this server. The number of digits in an extension number must match the entry in the Extension Length field for this server.

Adding a remote digital networking machine

About this task

You can add remote machines during initial system administration or at any time, as your network grows.

Note:

The messaging software accepts only one local machine. Do not attempt to add a second local machine. Use the instructions in this section only to add remote machines.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **Networked Servers**.

   The system displays the Manage Networked Servers page.
4. Click **Add a New Networked Server**.

   The system displays the Add Networked Server page.
5. Enter appropriate information for the fields on the Add Networked Server page.
6. Click **Save**.

Add Networked Server field description

Field	Valid Input	Description
Server Name	From 1 to 10 alphanumeric characters; can include dashes or underscores	Enter the name of the remote Communication Manager server. If the system is another Communication Manager server, you can determine the name

Table continues…

Field	Valid Input	Description
		on the remote Communication Manager server by selecting TCP/IP Administration menu option and then the Network Addressing window or web page. For the LDAP server type, the server name must be the same as the DNS name.
Server Type	tcpip=digital networking ldap=ldap/smtp networking	Enter the type of machine you are creating or changing.
IP Address	Four decimal numbers written in dotted format: each number needs to be in the range 0 to 255. For example, 135.9.52.45.	The IP address that is used when the messaging software connects to the remote machine to establish a call for digital networking.
Password	From 5 to 10 alphanumeric characters; can include dashes or underscores	The password sent to the remote machine when establishing a connection.
Voiced Name	yes, no	This field contains a no until you record a name for the system. This field automatically changes to yes when you record a name for the machine.
Send to Non-Administered Recipients	• If you select Yes, the Messaging system will attempt to deliver messages to non-administered remote recipients. • If you select No, the Messaging system will not attempt to deliver messages to non-administered remote recipients.	Use this drop-down list to enable or disable message delivery to non-administered remote recipients. The system displays this field only when the server tpe is TCPIP.
Mailbox Number Length	An integer from 3 to 10	Enter the length of extensions on the local system. The value you enter must match the extension length in your dial plan.
Voice ID	Display-only	Displays a system-assigned identifier that you must use to identify the machine if you decide to record machine names.
Default Community	An integer from 1 to 15	If you have administered your system to use community sending restrictions, enter the default community number for your subscriber population.
Updates In	yes, no	Select yes if the local system accepts updated database information from the remote system. The Updates In field must also be set to yes on the local Machine Profile screen.

Table continues…

Field	Valid Input	Description
		Set to yes only after testing the network end to end during initial administration.
Updates Out	yes, no	Select yes if the local system sends updated database information to the remote system. The Updates Out field must also be set to yes on the local Machine Profile screen. Set to yes only after testing the network end to end during initial administration.
Remote LDAP Port		Port that will be used when the system connects to this networked machine to send directory updates. For the local server, the default for this field is the port specified in the LDAP Directory Update Port field on the System Administration page. For a Networked Server, this field will only appear if the Server Type is ldap.
Inbound LDAP Security		Encryption type required for the connection between the messaging server and a remote networked machine for inbound LDAP directory updates. This field is disabled if the Updates In field is set to no. Attempts by remote networked machines to perform directory updates without using the specified level of security will be denied.
Outbound SMTP Port	Default=25	Port used when the network connects to this machine. This field is applicable only for an LDAP networked server.
Outbound SMTP Service	Default=SMTP (User TLS if available)	SMTP service type required for the connection between the messaging server and a remote networked machine. You can select from the following options: • SMTP (User TLS if available) to send messages that use SMTP to this networked server by using TLS if the remote machine can use TLS. • Secure SMTP (Using TLS) to send messages that use SMTP to this networked server by using TLS
Prefix	From 0 to 21 alphanumeric characters	Enter the prefix digits. A user enters the prefix before the remote subscriber's extension when addressing voice messages. To simplify this task, use a short, descriptive prefix. The

Table continues…

Field	Valid Input	Description
		total length of the prefix plus the extension must not exceed 24 characters. The system uses the prefix only to identify subscribers. It is not used for dialing out, so it does not need to match an area code or office code. The following are examples of possible prefixes: • No prefix . The prefix is required only when one or more of the remote subscribers share the same extension numbers as the local subscribers (the extension ranges of the two systems overlap). If there are no overlapping extension numbers, a prefix is not needed. • Public network access code . When addressing a message to a remote subscriber, the local subscriber enters the remote subscriber's number as if placing a call to that subscriber. • Location code . This method simplifies addressing messages by requiring only an alphanumeric code in front of the extension number. Location codes are shorter and often easier to remember.
Starting Mailbox Number	A 3-digit to a 50-digit string	Enter the starting extensions for the ranges of telephone numbers used on the remote system. (to designate a block of switch extensions for remote subscribers.) For example, if the system uses extensions between 2000 and 3000, enter 2000 in the **Start Extension** field. Up to 10 different ranges can be specified to pinpoint the exact set of extension blocks used by the remote system. The length of the start and end extension must agree with the **Extension Length** field. For a 5-digit extension, the default is from 00000 to 99999.
Ending Mailbox Number	A 3-digit to50-digit string	Enter the ending extensions for the ranges of telephone numbers used on the remote system. (to designate a block of switch extensions for remote subscribers.)

Table continues…

Field	Valid Input	Description
		For example, if the system uses extensions between 2000 and 3000, enter 3000 in the **End Extension** field.
Warnings	Display-only	This field displays a warning when a duplication or overlap of an extension range for another machine is being assigned.

Changing remote machine information

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. Log in to Communication Manager Messaging web page.
4. In the **Server Administration** section, click **Networked Servers**.

   The system displays the Manage Networked Servers page.
5. View the list of networked servers on this page.
6. Select a server that you want to edit, and click **Edit the Selected Networked Server**.

   The system displays the Edit Networked Server page.
7. Edit appropriate fields on the Edit Networked Server page, and click **Save**.

   Note:

   The **Voice ID** fields are display only. You cannot change the information in the fields.

Renaming a remote machine

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **Networked Servers**.

   The system displays the Manage Networked Server page.
4. Select a server and click **Edit the Selected Networked Server**.

   The system displays the Edit Networked Server page.
5. In the **Server Name** field, change the name of the server.

The name must be unique. The machine name can be up to 10 alphanumeric characters in length. The following rules apply:

- The machine name cannot contain blank (embedded) spaces. For example, denver 1is not allowed, but denver_1is allowed.
- The Machine Name field is a case-sensitive field. Uppercase letters must be entered as uppercase, and lowercase letters as lowercase.
- Hyphens (-) are allowed.
- Underscores (_) are allowed.
- The machine name cannot start with a number.

6. Click **Save**.

   The system displays a dialog box with the message:

   ```
   Server Information modified successfully.
   ```

   If you change the local machine profile, contact all remote network administrators and inform them about the changes.

Recording remote machine names

About this task

You can record the name of each remote voice mail system, telephone number, or range of machines and/or numbers by using your telephone. The local system voices these names when local subscribers address messages to a machine or when they receive messages from remote subscribers whose names are not recorded or who are not administered.

Procedure

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

   The system displays the Manage Subscribers page.
4. In the Local Subscriber row, click **Manage**.
5. Select the subscriber for whom you want to verify announcement control permission and click **Edit/Delete the Selected Subscriber**.
6. In the **Announcement Control** field, click **yes**.
7. View the remote machines on the Manage Subscribers page.
8. Record the Voice IDs of each system for which you want to record a name.

   Note:

   Some remote machine profiles are used for a range of machines. Either voice a name that is meaningful for all machines in the range or do not voice a name for these profiles.

9. Using a touchtone telephone, log in to the messaging system by using the extension that has announcement-control permissions.
10. From the Activity menu, press `9` to perform system administration.
11. Press **6** to record machine names.
12. Using the touchtone keypad, enter the voice ID for the first remote machine and press `#`.
13. At the tone, speak the remote machine's name.
14. Press `#` to approve the recording or press `* D` to delete and rerecord the name.
15. Repeat Step 6 through Step 8 for each remote system or telephone number name.
16. After recording all remote machine names, press `* R` to return to the Activity menu or hang up to exit the system.

Deleting remote machines

About this task

If you are informed that a remote machine has been removed from the network, you must delete that remote machine from your local machine. When you delete a remote machine, you also delete any remote subscribers who are associated with that remote machine. Machine information and subscriber information are not removed completely from the system until a nightly audit runs.

Because deleting a machine removes the remote machine and the remote subscribers assigned to that machine, before you proceed ensure that you really want to delete the machine, and then ensure that you enter the correct remote machine name. If you do make a mistake when removing a remote machine, you can restore the deleted remote machine before the nightly audit runs.

Note:

You cannot delete the local machine and messaging server, but you can change the settings of the local machine.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **Networked Servers**.

   The system displays the Manage Networked Servers page.
4. Select a server from the list, and click **Delete the Selected Networked Server**.

Retrieving a deleted remote machine

About this task

If you make a mistake by removing a remote machine, you can add the remote machine back to the system by running a series of audits. This procedure is possible only until the nightly audit on the day that you delete the machine. After the nightly audit runs, the deleted machine cannotbe retrieved.

Procedure

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

   The system displays the Audits page.
4. Click one of the following links:
   - **View Audit History**
   - **Audit Mailboxes**
   - **Audit Mailing Lists**
   - **Audit Voice Names**
   - **Audit Network Data**
   - **Audit Personal Directory Data**
   - **Audit Subscriber Data**
   - **Audit Nightly Data**
   - **Audit Weekly Data**

   After each audit, the system returns to the Audits page. See Voice Messaging Database Overview on page 198 for more information on these audits.

Listing address ranges for network machines

About this task

The Address Ranges screen displays a numerical list of address ranges that belong to all machines in the network. You can use this screen to determine if you have overlapping address ranges in your network. If you have overlapping address ranges, you must add a prefix for address ranges on the local or remote Machine Profile screens for any overlapping addresses.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **Networked Servers**.

   The system displays the Manage Networked Servers page.
4. Click **Display Report of Server Ranges**.

   The system displays the Report of Server Extension Ranges page with the address ranges of all the networked servers.

Report of Server Extension Ranges page field description

Field	Description
Server Name	Lists the name of each network server. **Note:** Each server name is a link you can click to go to the Edit Networked Server page. The Edit Networked Server page allows you to delete or change the settings for the networked server.
Prefix	Lists the address prefix of each server's extension range.
Starting Extension Number	Lists the starting extension number of each server's extension range
Ending Extension Number	Lists the ending extension number of each server's extension range.

Listing remote extensions

About this task

The Manage Remote Subscribers page displays a list of remote subscriber names, types, mailbox numbers, and the usage date.

Procedure

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

   The systems displays the Manage Subscribers page.
4. In the Remote Subscribers row, click **Manage**.

   The system displays the Manage Remote Subscribers page with a list of administered remote subscribers.

Manage Remote Subscribers page field descriptions

Field	Description
Mailbox Number	Extension of the remote subscriber
ASCII Name	Name of the remote subscriber if known
Type	Type of remote subscriber listed, administered, verified, or unverified
Usage Date	Last day the remote subscriber associated with this mailbox number had activity, was on the mailing list, or was the sender of a message not yet deleted
CID	Community ID for each remote subscriber

Viewing a list of machines

About this task

You can view of list of all the machines identified on the system, including the local machine and the administered remote machines.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **Networked Servers**.

   The system displays the Manage Networked Servers page. If you already have servers networked to your local messaging system, the details of the servers are displayed on this page.

Displaying Machine Information

Testing the digital networking and TCP/IP connection

Note:

Avaya is not responsible for the installation, administration, or test of communications between customer personal computers and the LAN. Customers need to seek service as directed by their LAN administrator to resolve problems with their LAN.

After you administer the digital networking and the TCP/IP connection, complete the following procedures to test digital networking:

- Sending a voice message to a remote user
- Receiving voice messages from remote test subscribers on page 136

Sending a voice message

About this task

For acceptance tests, you must administer two test subscribers for each remote machine. For example, if you plan to network with four remote machines named CB1, CB2, CB3, and CB4, you need to administer two test subscribers on each machine. During acceptance testing, you address voice messages to each of those test subscribers.

Procedure

1. Dial the voice messaging extension.
2. When prompted to enter an extension, use the telephone keypad to enter a local test subscriber extension followed by #.
3. Enter the password for the local test subscriber followed by #.
4. You hear the messaging Activity menu.
5. Press `1` to record a message.

6. At the tone, say the following:

   "This is a test message from <your name>. Please call me to verify that you have received this message. My number is <your number>."

7. Press # when you stop recording and approve the message.

   After you approve the message, you hear the following prompt:

   "Enter extension and pound sign. When finished addressing, press pound."

8. Enter the address for a remote test subscriber followed by #.

   The address includes the prefix, if any, and the extension of the remote test subscriber.

   After you press #, the remote machine repeats the remote test subscriber extension you entered.

9. Repeat Step 6 for each remote test subscriber on each remote machine.

10. When you complete entering remote test subscriber addresses, press #.

    You hear the following prompt:

    "To send message, press pound, or enter a delivery option. To hear a list of options, press 0."

11. Press # to send the message.

    The system schedules the delivery and returns you to the activity menu.

12. Hang up the telephone.

Receiving voice messages from remote test subscribers

About this task

Have remote test subscribers send messages to your local test subscribers during acceptance testing. You must retrieve the messages to verify that your local machine is administered correctly with the remote machines and is receiving messages correctly. When you retrieve the messages, you should hear the system say the name of the remote machine and the remote test subscriber, if you recorded a name for the remote machine and the remote test subscriber.

After you receive messages from the remote machines, contact each of the remote machine network administrators and inform each one that you received a message from their machine.

To retrieve messages from the test remote subscribers:

Procedure

1. Dial the voice messaging extension.

   This is the extension subscribers call to retrieve and send messages.

2. When prompted to enter an extension, use the telephone keypad to enter a local test subscriber extension followed by #.

3. Enter the password for the local test subscriber followed by #.

You hear the subscriber's name and a message telling you the number of messages in your mailbox, if any.

Messaging then plays the activity menu.

4. Press 2 to retrieve messages.
5. The messaging software plays the header for the first message.

   The header includes the name or extension of the sender and the date and time the message was received.
6. Press 0 to listen to the message.
7. As you listen to the message, note the remote machines and remote test subscribers that were able to exchange messages with you.
8. At the end of the message, you hear the following prompt:

   "To respond or forward, press one. To delete, press star d. To skip, press pound."
9. Press * 3, which is the same as * D, to delete the message.
10. Repeat Step 4 through Step 7 for each message in the local test subscriber's mailbox.
11. When you finish retrieving messages from remote test subscribers, hang up the telephone and then contact the remote machine network administrators and inform them that you received a message from their machine.

Remote user administration

Remote users are subscribers on remote Communication Manager Messaging systems who exchange messages with the subscribers on your system. Administering remote subscribers enables the local messaging system to send messages when a local subscriber records a message and addresses the message to a remote extension.

Important:

You must perform remote user administration to keep the list of remote subscribers on your system up to date.

Types of remote users

Remote messaging users are of the following types:

- Administered remote users:

  Administered remote users are users whom you have defined as remote users within the messaging system. Define remote users when you:

  - Conduct remote updates. See Overview of Remote Updates on page 138 for more information.
  - Manually administer a remote user instead of waiting for a remote update. See Administering a Remote User Manually on page 143 for more information.

LDAP/SMTP subscribers are always administered remote users. Unverified and verified remote users do not apply for LDAP/SMTP subscribers.

- Unverified remote users

  Unverified remote users are remote users who are unknown to the local messaging system. Unverified remote users automatically become administered remote users when the system goes through the remote update process.

- Verified non-administered remote users

  Verified non-administered remote users are remote users who appear in the local messaging database only because they have successfully exchanged messages with the local system. You must periodically check the List Remote Extensions screen to locate any verified remote users. See Viewing the Remote Extensions List on page 141. If a local user regularly exchanges messages with a verified remote user, you might want to administer the remote user.

Overview of remote updates

Remote updates provide an automatic method of administering remote users. Remote updates:

- Let you automatically add all remote users who need to exchange messages across the network.
- Let your local messaging system exchange user information with each remote messaging system that is administered on the local system.

Remote updates greatly reduce the time required to set up the messaging digital network. Whether you use the remote updates feature depends on the:

- Number of users in your network.
- Size and disk space of your local system.
- Number of networking ports that you are using.

You can also enter remote user information manually. Before you administer your user or remote update information, consult with the remote system administrators in your network. Each remote system administrator must determine whether to use remote updates.

Types of Remote Updates

The following types of remote updates are available:

- Complete updates
- Partial updates

Complete Updates

With a complete update, all user information is exchanged between systems. When a new system is added to the network, each existing system must request a complete update from the new system to add the new users to the network. Complete updates might involve thousands of users and require heavy system resources. Therefore, it is strongly recommended that you perform complete updates during nonprime time to reduce the impact on system users.

Additionally, the local messaging system can automatically schedule a complete update during nonprime time from a remote system if the local system detects discrepancies among databases.

Partial Updates

Partial updates occur on a regular basis to add or change information for users. For example, a partial update occurs when a new user is added to a remote system or a local system.

If all systems in the network allow updates, then any time a user is added to, deleted from, or changed on a system, that system notifies each system in the network.

Setting up remote updates for your local system

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **Networked Servers**.

   The system displays the Manage Networked Servers page. If you already have servers networked to your local messaging system, the details of the servers are displayed on this page.
4. Select the server for which you want enable remote updates for you local system.
5. Click **Edit the Selected Networked Server**.

   The system displays the Edit Networked Server page.
6. In the **Update In** and **Update Out** fields, click `yes` to set up remote updates for your Messaging server.
7. Click **Save**.

Setting up remote updates with specific remote systems

About this task

After you define the remote update capabilities for the local system, you must define the remote update capabilities of each remote system.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Administration** section, click **Networked Servers**.

   The system displays the Manage Networked Servers page. If you already have servers networked to your local messaging system, the system displays the details of the servers on this page.

Tip:

On the Manage Networked Servers page, you see a list of remote systems. See Viewing the Machine Lists on page 135.

4. Select the server you want enable remote updates for you local system.
5. Click **Edit the Selected Networked Server**.

   The system displays the Edit Networked Server page.
6. In the **Update In** and **Update Out** fields, click `yes` to set up remote updates for your Messaging server.
7. Click **Save**.

Running a remote update manually

About this task

You might need to run a remote update manually to populate the user database quickly or to correct database inconsistencies that were discovered during an audit.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.

   The system displays the Measurements page.
4. In the **Type** field, click **Feature**.
5. In the **Cycle** field, click **Daily**.
6. Click **Get Report**.
7. Write down the current number of remote users.
8. In the **Server Administration** section, click **Request Remote Update**.

   The system displays the Request Remote Update page
9. Select a server name from the drop-down menu.

   The Request Update button, which remains grey before this action is now active.
10. Click **Request Update**.

Tip:

You can know the status of an update by using the **Refresh Update Status** button. The current status is reflected: pending or competed with the time stamp.

Note:

The update might take some time, possibly hours, depending on the number of users on the remote system. Avoid running the remote update during prime time hours.

11. When the remote update is complete, in the **Messaging Administration** section, click **Subscriber Management**.

    The networked machines are listed under Remote Subscribers on the Manage Subscribers page.

12. To view the remote subscribers for which you recently did the update, click **Manage** provided for that machine.

    The system displays the Manage Remote Subscribers page. Check that the remote users are listed on the local system.

13. Now, go back to measurements page to confirm the number of remote users.
14. In the **Logs** section, click **Administrator**.

    The system displays Administrator's Log page.

15. Click **Display** to get the logs.
16. View the Administrator's Log to verify that no conflicts or problems occurred with the remote update.

Result

This ensures that the manual process of remote updates was successful.

Viewing the list of remote subscribers

About this task

Use the Manage Remote Subscribers to locate verified non-administered remote users and evaluate the usage dates of remote users. Although there is a record of the user, the system does not have a record of the name, name recording, and other information.

To determine how often messages are sent to a user, check the **Usage Date** column on the Manage Remote Subscribers page. Use the field to determine if you can delete any administered remote users. If the **Usage Date** column shows a current date, then the remote administered user exchanges messages with someone on the local system and should not be removed.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Subscriber Management**.
4. Click **Manage** next to a machine listed under Remote Subscribers.

Tip:

On the Manage Networked Servers page, you see a list of remote systems. See Viewing the Machine Lists on page 135.

The Manage Remote Subscribers page also lists the networked machine names.

The system displays the Manage Remote Subscribers page. For the machine you selected, the screen lists the following types of remote users:

- Administered
- Verified nonadministered remote users
- Unverified nonadministered remote users

5. Check the usage dates for both verified users and administered users.

   If a verified user has a recent usage date, perhaps within the last month, you might want to administer the user and record the user's name.

   See Recording Remote User Names on page 146 for more information.

Setting automatic deletion of non-administered remote users

About this task

You can use the Non-Administered Remote Subscriber Option page to request that non-administered remote users be deleted automatically.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Non-Admin Remote Subs**.
4. The system displays the Non-Administered Remote Subscriber Option page.
5. Provide appropriate inputs in the **Days Without Activity** and **Even if on Mailing List?** fields.
6. Click **Update Options**.

Non-Administered Remote Subscriber Options field descriptions

Name	Description
Days without Activity	The number of days after which non-administered remote subscribers are automatically removed if there is no send/receive activity between the remote subscriber and a messaging subscriber. A value of 0 will turn off the automatic deletion of remote subscribers. You can enter a number from 0 to 999 in this field.

Table continues…

Name	Description
Even if on a Mailing List?	Select Yes to delete the remote subscriber from the system database after the administered number of days of inactivity. Select No to accept nonadministered remote subscribers who are on mailing lists from the automatic deletion. When you select No, the system searches through all messaging subscribers' mailing lists for a non-administered remote subscriber address. If a non-administered remote address is found on a mailing list, the system does not delete the address, even if there was no send/receive activity between the remote subscriber and messaging for the amount of time entered above.

Manual administration of a remote user

Running a remote update can use one of your networking ports for quite some time. If you want to administer a remote user immediately but do not want to run a remote update, you might want to administer that user manually.

You can perform the following remote user tasks manually:

- Add a remote user on page 143
- Change a remote user on page 145
- Delete a remote user on page 145

Adding a Remote User manually

About this task

Running a remote update can use one of your networking ports for quite some time. If you want to add a remote user immediately but do not want to run a remote update, you can add that user manually.

Procedure

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

   Tip:

   On the Manage Subscribers page, you see a list of remote systems. See Viewing the Machine Lists on page 135.
4. Click **Manage** next to a machine listed under Remote Subscribers.

   The system displays the Manage Remote Subscribers page.
5. Provide appropriate values in the fields on the Manage Remote Subscribers page.
6. Click **Save**.

Add Remote Subscriber field descriptions

Field	Description
Common Name	The name of the remote user to be added or changed. This is a mandatory input field; there is no default value. The name must be unique and can be a string of 1 to 29 alphabetic characters, including dashes or underscores. It is recommended that you enter the last name first and then a comma and then the first name. For example: Doe,Jane. However, any combination of letters can be used. Notice that there are no blank (embedded) spaces in the example. That is, the name is not entered as Doe, Jane. Furthermore, in areas in which telephones have letters that accompany the numbers, each name must be unique as entered on the keypad of a touchtone telephone. For example, use Doe,JaneA and Doe,JaneZ to distinguish between two subscribers named Jane Doe.
Mailbox Number	The user's telephone extension. The extension can be a 3-digit to 50-digit telephone extension. The extension must: • Be within the range of numbers assigned to the remote machine. • Not be assigned to another user on the same remote machine. The address (prefix plus extension) must be a unique address among all networked machines. • Be of the length administered on the remote machine.
Trusted Server of or Machine Name	The name of the machine on which the remote user is administered, if the user is an administered user. Only an administered or a verified subscriber can select a machine. This is a display-only field that cannot be changed.
Community ID	Enter the community ID to be assigned to this user. A community is a group of users that is restricted from sending messages to other designated groups. For more information on community sending restrictions, see Setting Up Community Sending Restrictions on page 72. If this field is left blank, the system default community ID from the Machine screen for the local machine is used. If sending restrictions are in place on your network, the Community ID for this user must be the same on this machine as on the user's local machine.
Administered	When you manually add a remote user, the system automatically places a y in the field. Also, if a non-administered remote user becomes administered through a remote update, the value in this field changes from n to y. If a remote system calls the local system and sends a message from a non-administered remote user, the local system creates a verified remote user record in the database and places an n in the field.
Voiced Name	This field contains an n until you record the user's name or until the user's voiced name comes across from the user's local machine during an update.

Table continues…

Field	Description
	This field automatically changes to y when you record the user's name or when the user's voiced name comes across from the user's local machine during an update.
Non-Administered Type	This field displays the type of nonadministered user, such as verified.
Last Usage Date	This field displays the most recent date the remote user received a message. The field helps you to determine the call traffic for the user.

Changing remote user data manually

About this task

Running a remote update can use one of your networking ports for quite some time. If you want to change a remote user immediately but do not want to run a remote update, you can change that user manually.

Procedure

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

   The system displays the Manage Subscribers page.

   The system displays networked servers under Remote Subscribers.

   Tip:

   On the Manage Networked Servers page, you see a list of remote systems. See Viewing the Machine Lists on page 135.
4. Click **Manage** next to a machine listed under Remote Subscribers.

   The system displays the Manage Remote Subscribers page.
5. Select the remote subscriber whose information you want to change, and click **Edit the Selected Subscriber**.

   The system displays the Edit Remote Subscriber page.
6. Complete or change the fields on this screen.
7. Click **Save**.

Deleting a remote user manually

About this task

Running a remote update can use one of your networking ports for quite some time. If you want to delete a remote user immediately but do not want to run a remote update, you can delete that user manually. For example, to conserve system resources, you might want to delete an administered remote user with an old Last Usage date.

Note:

Mailing lists often include administered remote users. If you manually delete a remote user, the user's name is then removed from mailing lists with no notification to the user or the mailing list owner.

Procedure

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

   The system displays the Manage Subscribers page.

   The system displays networked servers under Remote Subscribers.

   Tip:

   On the Manage Networked Servers page, you see a list of remote systems. See Viewing the Machine Lists on page 135.
4. Click **Manage** next to a machine listed under Remote Subscribers.

   The system displays the Manage Remote Subscribers page.
5. Select a remote subscriber, and click **Delete the Selected Subscriber**.

Recording Remote User Names

Recording a remote user's name

About this task

To ensure that any new or changed recorded name is updated, you must:

- Set the **Updates In** field to **y** on the Edit Messaging Server page and the Edit Networked Server page.
- Set the **Updates Out** field to **y** on the Edit Networked Server page.

Procedure

1. From any telephone, log in to the messaging administrator's mailbox.
2. Press `9` to access the system administrator's menu.
3. Press `4` to record the remote user names.

   The system plays the following message:

   `Enter remote user extension and pound sign.`
4. Enter the extension for the remote user and press `#`.
5. At the tone, speak the user's name.

6. Before you approve the recording, you can do the following:
   - Press `2 3` to listen to the remote user name recording.
   - Press `2 1` to record the remote user name again.
   - Press `* D` to delete the remote user name recording.
7. When you are satisfied with the quality of the recording, press `#` to approve it.
8. Repeat Step 4 to Step 7 to record the next remote user's name.
9. When you finish recording all remote user names, hang up the telephone.

Verify a user's name recording

About this task

To verify that you have successfully recorded a user's name:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Subscriber Management**.
4. Click **Manage** next to a machine listed under Remote Subscribers.

   The system displays the Manage Remote Subscribers page.
5. Select the remote subscriber whose information you want to change, and click **Edit the Selected Subscriber**.

   The system displays the Edit Remote Subscriber page.
6. Verify that the **Voiced Name?** field contains the value **y**.
7. Click **Save**.

Result

You can verbally record remote user names into the system. Then, when a local user addresses a message to a remote user, the system plays back the remote user's name as a friendly confirmation.

Note:

If you use the Remote Updates feature and a name was recorded for the user on the remote system, the recorded name is updated on the local system as part of the remote update. See Overview of Remote Updates on page 138 for more information.

Customizing announcements overview

Voice prompts or announcements inform users about the actions they must perform. Use the commands and procedures described in this topic to change messaging announcements.

To customize messaging announcements, you can use fragments, announcements, and announcement sets.

Fragments

The voice prompts you hear in messaging consist of one or more pieces of recorded text called fragments.

A fragment is a recorded word, phrase, or sentence. Each fragment is identified by a number prefaced by the letter "f".

For example, the voice prompt "Previous login incorrect. Please reenter extension and pound sign," contains these two fragments:

- f233 "Previous login incorrect. Please reenter extension,"
- f224 "and pound sign."

Announcements

An announcement is a placeholder within the system for playing fragments. Each announcement is identified by a number prefaced by the letter a. For instance, a10 is announcement 10. Each event that can occur within messaging has one or more announcement numbers permanently assigned to it. Fragment numbers are then assigned to the announcement numbers.

Thus, when a caller or subscriber completes an event, such as pushing a button, messaging processes the announcement number assigned to that event and then plays the fragments assigned to that announcement.

See Example: How an Announcement Links Voice Fragments to Events on page 150 for a sample event sequence. In this example, announcement a815 marks a place to play fragments when a caller connects to messaging. The standard voice prompt at this point is a welcome message. As the caller continues to press more keys, additional announcements trigger the messaging software to play the assigned fragments.

Announcements are fixed in place. You cannot use an announcement number to mark a different point in the event sequence. Therefore, you cannot add, change, or delete an announcement number. However, you can add, change, or delete fragments assigned to announcements and thereby change announcements.

See Commonly Customized Fragments and Announcements on page 150 for a list of commonly changed announcements.

Announcement sets

An announcement set is a collection of announcements. These can be standard or custom announcements.

Standard Announcement Sets

The messaging software offers standard announcement sets in several languages. For more information about installing Announcement Sets, see the *Communication Manager Messaging Alarms and Events Guide*. The standard set is loaded and activated by default.

Note:

If the standard version is English, your system comes with two announcement sets: a standard version and a terse version. The terse version contains all of the announcements in the standard set, but individual announcements contain fewer words. For example, the standard US

version of announcement a2 is: Partial entry deleted. The terse version is: deleted. You can also create and activate custom announcements for the terse set.

Custom announcement sets

To create a custom announcement set, you add an announcement set name to the system and then copy into that set the announcements from another standard or custom set. You can then change the announcements and fragments in the newly created custom set and activate it.

Active and administrative announcement sets

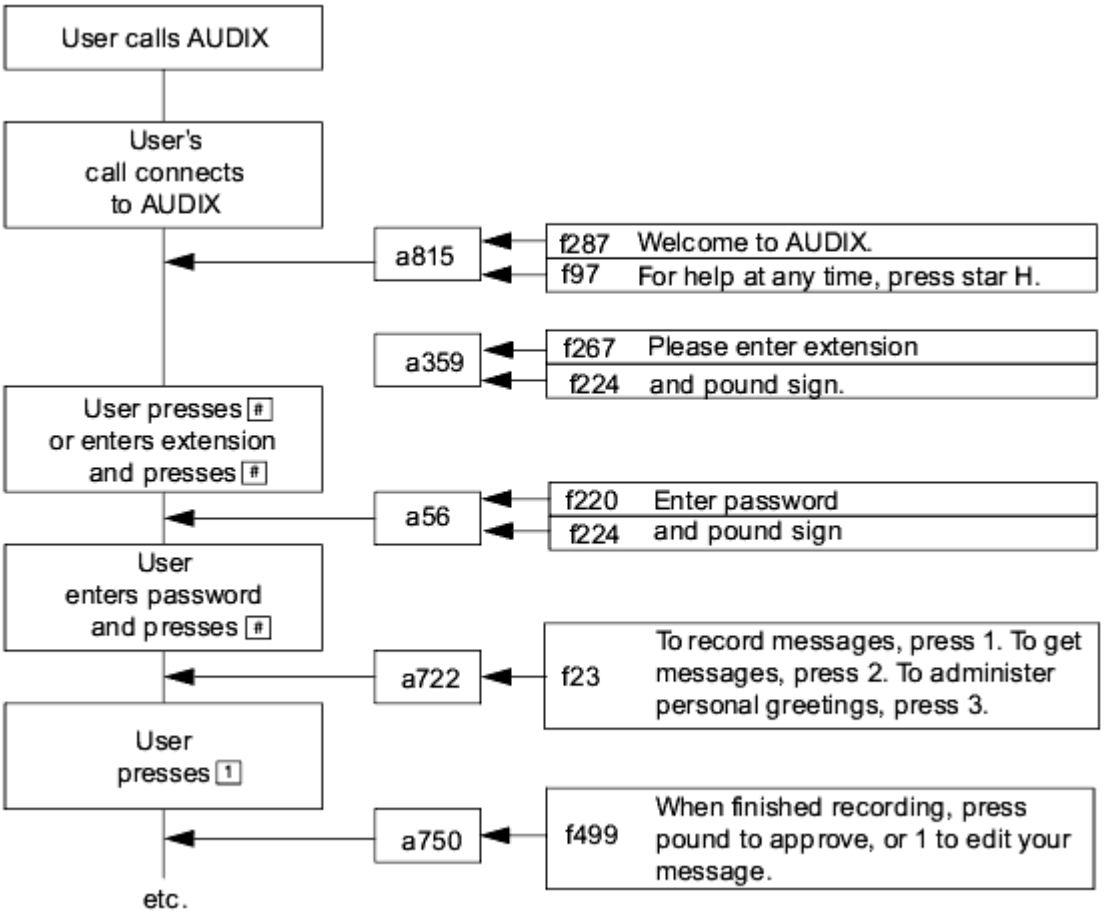
The standard announcement set is the default active announcement set. Active means that the messaging software currently plays the set's announcements to users. You can also designate an announcement set as the administrative announcement set. Administrative means that you can record in the set. The administrative set might not be the active announcement set. If the same announcement set is both active and administrative, any recorded changes made to the administrative version are also made automatically to the active version.

If your announcement set is US English, you may want to replace the standard version with the terse version as the active announcement set. See Activating an Announcement Set on page 165 if you want to designate terse as the active announcement set.

Installation of other languages

For information about obtaining and installing another language announcement set, contact your account executive.

Example: How an Announcement Links Voice Fragments to Events



Commonly Customized Fragments and Announcements

To effectively customize your announcements, you must know the fragment numbers and the context in which they are most commonly used. This topic provides that information.

Fragments and announcements combine to tell subscribers and callers what to do and what their options are for using the system. You can change Communication Manager Messaging announcements to meet the needs of the business and of the subscribers.

List of Commonly Customized Fragments and Announcements

The fragments listed in the following table are the most commonly customized fragments. Each fragment is listed with one of the announcements that contains it to show the context in which the fragment is normally used. In addition to the announcements listed in this section, the system also uses most of the fragments in other announcements. However, any other announcements that use a fragment have a construction very similar to the announcements listed here.

The announcements and fragments listed apply to US English, US English TDD, and US English 1-2-3. However, 1-2-3 fragments use numbers to identify touchtone keys, not letters. Also, you must rerecord TDD fragments with a teletypewriter (TTY) connected to your telephone.

Announcement Number	Fragment Number	Fragment Text
a18	f555	To access your mailbox, press star R.
f291	To transfer to another extension, press star T.	
f80	To have system wait, press star W. If finished, please hang up or to disconnect messaging, press star star X.	
a119		IF(VERSION>2)THEN
f305	You are at the activity menu.	
	IF(NUMBER==0)THEN	
f990	To record and send voice mail messages, press 1.	
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF	
f992	To get messages, press 2.	
f996	To check your outgoing messages, press 4.	
	a1174(NUMBERNUMBER(2)NUMBER(3)IF(NUMBER==0)THEN	
f1001	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ELSE	
f1165	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ENDIF	
	f282	To have system wait, press star W. To access the names or number directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.
	ELSE	
f305	You are at the activity menu.	

Table continues…

Announcement Number	Fragment Number	Fragment Text
f985	To record and send voice mail messages, press 1. To get messages, press 2.	
f48	To check your outgoing messages, press 4. To administer mailing list, personal directory, password, or account name, press 5. To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
f282	To have system wait, press star W. To access the names or number directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.	
a174		NAME
f822	As you use messaging your name will be included in system announcements that you and other people will hear. At the tone, please speak your name. After speaking your name, press one.	
a199	f592	Messaging passwords must now be NUMBER
f81	digits.	
f593	Please choose a new password of NUMBER(2)	
f81	digits.	
f173	Please enter new password	
f224	and pound sign.	

a289		IF(VERSION>2)THEN (where v. 3 has call answerdisable)
		a1178(NUMBER
		NUMBER(2)NUMBER(3)NAME)ELSE
		IF(NUMBER==0)THEN

Table continues…

Announcement Number	Fragment Number	Fragment Text
f43	Your call is being answered by messaging. NAME	

f44	is not available. To leave a message, wait for the tone.
	ENDIF
	IF (NUMBER==1)
	THEN	

	f71	To leave a message, wait for the tone. ENDIF IF (NUMBER==2) THEN NAME
f44	is not available. To leave a message, wait for the tone. ENDIF	
a349	f118	Enter last name
f224	and pound sign.	
f175	Please note only messaging subscribers can be specified by name.	
a514	f582	Messaging passwords must now be at least NUMBER
f81	digits.	
f593	Please choose a new password of NUMBER(2)	
f588	or more digits.	
f173	Please enter new password	
f224	and pound sign.	
a584	f186	To record messages, press 1. To get messages, press 2. To check you outgoing messages, press 4.
a728	f775	To record messages, press one. To get messages, press two. To

Table continues…

Announcement Number	Fragment Number	Fragment Text
		administer personal greetings, press 3.
a815	f287	Welcome to messaging.
f97	For help at anytime, press star H.	

a1174		IF(NUMBER==0)THEN
		IF(NUMBER(2)==0)THEN
		IF(NUMBER(3)==0)THEN

f997	To administer mailing list, personal directory, password, or account name, press 5.	
	ELSE	
1149	To administer mailing list, personal directory, password, account name, or call answer options, press 5.	

	ENDIF
	ELSE
	IF(NUMBER(3)==0)THEN	

f1147	To administer mailing list, personal directory, password, account name, or addressing options, press 5.	
	ELSE	
	f1151	To administer mailing list, personal directory, password, account name, addressing options, or call answer options, press 5.

	ENDIF
	ENDIF
	ELSE
	IF(NUMBER(2)==0)THEN
	IF(NUMBER(3)==0)THEN	

f999	To administer mailing list, personal directory, password, or account name, press 5.	
	ELSE	
f1150	To administer mailing list, personal directory, password, account	

Table continues…

Announcement Number	Fragment Number	Fragment Text
	name, or call answer options, press 5.	

	ENDIF
	ELSE
	IF(NUMBER(3)==0)THEN	

f1148	To administer mailing list, personal directory, password, account name, or addressing options, press 5.	
	ELSE	
f1146	To administer mailing list, personal directory, password, account name, addressing options, or call answer options, press 5.	
a1178		IF(NUMBER==0)THEN IF(NUMBER(3)==1)THEN (where 1=call answer disabled)
f43	Your call is being answered by messaging.	
	NAME	
f1163	is not available.	
f1162	Sorry, the mailbox you have reached is not accepting messages at this time.	
f95	Please disconnect.	
	ELSE	
f43	Your call is being answered by messaging.	
	NAME	
f44	is not available. To leave a message, wait for the tone.	

	ENDIF
	ENDIF
	IF(NUMBER==1)THEN
	IF(NUMBER(3)==1)THEN (where 1=call answer disabled)	

f1162	Sorry, the mailbox you have reached is not accepting messages at this time.	

Table continues…

Announcement Number	Fragment Number	Fragment Text
	f95	Please disconnect.
	ELSE	
f71	To leave a message, wait for the tone.	

	ENDIF
	ENDIF
	IF(NUMBER==2)THEN
	IF(NUMBER(3)==1)THEN (where 1=call answer disabled)	

	NAME	
f1163	is not available.	
f1162	Sorry, the mailbox you have reached is not accepting messages at this time.	
f95	Please disconnect.	
	ELSE	
	NAME	
f44	is not available. To leave a message, wait for the tone.	

		ENDIF
		ENDIF
		IF(NUMBER(2)==1
		&&
		NUMBER(3)!=1)THEN

f1141	When finished recording, press pound for more options.	
a2077	f305	You are at the activity menu.
	IF(NUMBER == 0) THEN	
f990	To record and send voice mail messages, press 1.	
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF,	
f992	To get messages, press 2.	

Table continues…

Announcement Number	Fragment Number	Fragment Text
f1006	To record or change the greeting heard by callers, press 3.	
f996	To check your outgoing messages, press 4.	
f2041	To customize your mailbox. For example, to create or edit your mailing lists, to specify your printer preferences, or to change your password, press 5.	
		IF(NUMBER == 0) THEN
f1001	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ELSE	
f1165	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ENDIF,	
f282	To have system wait, press star W. To access the names or numbers directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.	
a2079	f305	You are at the activity menu.
	IF(NUMBER == 0) THEN	
f990	To record and send voice mail messages, press 1.	
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF,	
f992	To get messages, press 2.	
	f1016	To administer your greeting, press 3.
f996	To check your outgoing messages, press 4.	

Table continues…

Announcement Number	Fragment Number	Fragment Text
f2041	To customize your mailbox. For example, to create or edit your mailing lists, to specify your printer preferences, or to change your password, press 5.	
	IF(NUMBER == 0) THEN	
f1001	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ELSE	
f1165	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ENDIF,	
f291	To transfer to another extension, press star T.	
f282	To have system wait, press star W. To access the names or numbers directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.	
a2081	f305	You are at the activity menu.
	IF(NUMBER == 0) THEN	
	f990	To record and send voice mail messages, press 1.
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF,	
f992	To get messages, press 2.	
f1006	To record or change the greeting heard by callers, press 3.	
f996	To check your outgoing messages, press 4.	
f2041	To customize your mailbox. For example, to create or edit your	

Table continues…

Announcement Number	Fragment Number	Fragment Text
	mailing lists, to specify your printer preferences, or to change your password, press 5.	
	IF(NUMBER == 0) THEN	
f1001	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ELSE	
f1165	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ENDIF,	
	f291	To transfer to another extension, press star T.
f282	To have system wait, press star W. To access the names or numbers directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.	
a2082	f305	You are at the activity menu.
	IF(NUMBER == 0) THEN	
f990	To record and send voice mail messages, press 1.	
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF,	
f992	To get messages, press 2.	
f996	To check your outgoing messages, press 4.	
f2041	To customize your mailbox. For example, to create or edit your mailing lists, to specify your printer preferences, or to change your password, press 5.	
	IF(NUMBER == 0)	

Table continues…

Announcement Number	Fragment Number	Fragment Text
	THEN	
	f1001	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.
	ELSE	
f1165	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ENDIF,	
f282	To have system wait, press star W. To access the names or numbers directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.	
a2084	f305	You are at the activity menu.
	IF(NUMBER == 0) THEN	
f990	To record and send voice mail messages, press 1.	
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF,	
f992	To get messages, press 2.	
f1006	To record or change the greeting heard by callers, press 3.	
	f996	To check your outgoing messages, press 4.
f2041	To customize your mailbox. For example, to create or edit your mailing lists, to specify your printer preferences, or to change your password, press 5.	
	IF(NUMBER == 0) THEN	
f1001	To change outcalling information, press 6. To scan incoming	

Table continues…

Announcement Number	Fragment Number	Fragment Text
	messages automatically, press 7. To re-logon, press star star R.	
	ELSE	
f1165	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ENDIF,	
f291	To transfer to another extension, press star T.	
f117	To reach the covering extension, press star zero.	
f282	To have system wait, press star W. To access the names or numbers directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.	
a2085	f305	You are at the activity menu.
	IF(NUMBER == 0) THEN	
	f990	To record and send voice mail messages, press 1.
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF,	
f992	To get messages, press 2.	
f996	To check your outgoing messages, press 4.	
f2041	To customize your mailbox. For example, to create or edit your mailing lists, to specify your printer preferences, or to change your password, press 5.	
	IF(NUMBER == 0) THEN	
f1001	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	

Table continues…

Announcement Number	Fragment Number	Fragment Text
	ELSE	
f1165	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ENDIF,	
f291	To transfer to another extension, press star T.	
	f282	To have system wait, press star W. To access the names or numbers directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.
a2086	f305	You are at the activity menu.
	IF(NUMBER == 0) THEN	
f990	To record and send voice mail messages, press 1.	
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF,	
f992	To get messages, press 2.	
f1006	To record or change the greeting heard by callers, press 3.	
f996	To check your outgoing messages, press 4.	
f2041	To customize your mailbox. For example, to create or edit your mailing lists, to specify your printer preferences, or to change your password, press 5.	
	IF(NUMBER == 0) THEN	
	f1001	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.
	ELSE	

Table continues…

Announcement Number	Fragment Number	Fragment Text
f1165	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ENDIF,	
f291	To transfer to another extension, press star T.	
f117	To reach the covering extension, press star zero.	
f282	To have system wait, press star W. To access the names or numbers directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.	
a2087	f305	You are at the activity menu.
	IF(NUMBER == 0) THEN	
f990	To record and send voice mail messages, press 1.	
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF,	
	f992	To get messages, press 2.
f996	To check your outgoing messages, press 4.	
f2041	To customize your mailbox. For example, to create or edit your mailing lists, to specify your printer preferences, or to change your password, press 5.	
	IF(NUMBER == 0) THEN	
f1001	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ELSE	
f1165	To change outcalling information, press 6. To scan incoming	

Table continues…

Announcement Number	Fragment Number	Fragment Text
	messages automatically, press 7. To re-logon, press star star R.	
	ENDIF,	
f291	To transfer to another extension, press star T.	
f117	To reach the covering extension, press star zero.	
f282	To have system wait, press star W. To access the names or numbers directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.	
a2088	f305	You are at the activity menu.
	IF(NUMBER == 0) THEN	
f990	To record and send voice mail messages, press 1.	
	ELSE	
f991	To record and send voice mail, press 1.	
	ENDIF,	
f992	To get messages, press 2.	
f1006	To record or change the greeting heard by callers, press 3.	
f996	To check your outgoing messages, press 4.	
f2041	To customize your mailbox. For example, to create or edit your mailing lists, to specify your printer preferences, or to change your password, press 5.	
	IF(NUMBER == 0) THEN	
f1001	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.	
	ELSE	

Table continues…

Announcement Number	Fragment Number	Fragment Text
	f1165	To change outcalling information, press 6. To scan incoming messages automatically, press 7. To re-logon, press star star R.
	ENDIF,	
f282	To have system wait, press star W. To access the names or numbers directory, press star star N. If finished, please hang up or to disconnect messaging, press star star X.	

Activating an announcement set

Procedure

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

   The system displays Administer System Attributes and Features page.

   Note:

   You can list all available announcement sets.
4. In the **System** field, under **ANNOUNCEMENT SETS**, click the announcement set that you want to activate.

   After you activate the announcement set, subscribers and callers will hear announcements in the announcement set.
5. Click **Save**.

Listing Announcement Sets

About this task

List announcement sets to determine:

- The names that are in use for announcement sets
- Whether you added or removed an announcement set successfully
- The sets that are available for copying

To display a list of existing announcement sets:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Announcement Sets**.

   The Announcements Sets page displays the list of existing sets.

Account Code Billing administration

Account Code Billing gives you the ability to assign Communication Manager server account codes to calls originated by Communication Manager Messaging voice ports. With this Account Code Billing, you can track the expense of outbound calls, message notification calls, and other types of calls. Account codes are not recorded by the switch for internal calls.

You must administer account codes on your Communication Manager server system before you can use Account Code Billing for messaging calls. See the Communication Manager Administration documentation for detailed instructions on administering account codes.

Administration process and uses

This section contains the following tasks for administering Account Code Billing for Communication Manager Messaging calls:

- Defining the Dialing Sequence
- Assigning Account Codes
- Testing the Dialing Sequence

Account Code Billing is used primarily with the following messaging features:

- Outcalling
- (Deprecated) Message Manager

Account codes are applied to all outbound calls placed by individual messaging subscribers. This includes:

- Message notification outcalls
- Call delivery messages

The account code is included in the Communication Manager server station message detail recording (SMDR) record. Communication Manager server system administrators can specify filters to determine which calls (for example, local or long distance) produce a call detail recording (CDR) record.

System requirements

To use the Account Code Billing feature, you must have a Call Accounting System (CAS) to interpret CDR or SMDR data

Defining the dialing sequence

The switch begins to record account code information for a given call when it receives an account code feature access code (FAC). The FAC must be received in the correct order in the sequence of digits dialed. This assures that the switch receives a signal to record the account code before the account code is sent to the switch. In other words, the messaging software must send the FAC, account code, call destination, and other digits to the switch in the correct sequence. This sequence varies depending on the telephone system and the application. Therefore, you must administer a dialing sequence for the Account Code Billing feature. This sequence is defined on the Outgoing Call Sequence screen.

Administering a Dialing Sequence

About this task

To administer a dialing sequence:

Procedure

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

   The system displays the Dial Sequences page.
4. In the **Dialing Sequence** field, type uppercase `N`.

   The default Dial Sequences page, does not contain active account code.
5. In the left navigation pane, under the **Diagnostics** group, click **Test Outgoing Call Sequence**.

   The system displays the Test Outgoing Call Sequence page.
6. Type appropriate values in the fields and click **Run Test**.

Result

Note:

If you are using the Outcalling feature, the subscriber might include the account code FAC and account code in the dial string for message notification. In this case, the FAC, account code, and notification number are all part of the destination number. When the system constructs the dialing sequence, the account code appears twice, once as the account code and once as part of the destination number. To avoid this duplication of account codes, it is recommended that subscribers be instructed not to include the account code as part of the dial string for message notification.

However, if subscribers are including authorization codes in the dial string for message notification, there is no conflict with account codes. Subscribers can continue to include the authorization codes.

Test Outgoing Call Sequence field descriptions

Field Name	Valid Input	Description
Port Number	Any port number less than or equal to the number of ports purchased	The field allows you to direct a test call to a specific voice port. It can be used to detect problems that arise from different restriction levels among voice ports. This field is optional. If no value is entered, any available port will be used.
Mailbox to be Tested	Any valid mailbox number	This field allows you to specify a subscriber's mailbox for the test. This subscriber's account code is included in the **Dialed Digits:** field.
Destination Number	A combination of: • Any valid on-premises, local, long distance, or international telephone number • Any additional commands, listed at right	A Destination Number must be specified for this test to run.

Dialing Sequence Example

Note:

You must include an uppercase Nin the dialing sequence. If Nis not present in the dialing sequence, the Outcalling feature will not function.

The Communication Manager server requires the account code FAC to be sent before the account code is sent. For the Communication Manager server, the account code FAC is set during the process of administering account codes on the switch. You must know this FAC before you can set the dialing sequence.

The following dialing sequence sends account codes from the messaging voice ports to the Communication Manager server. In this sequence, *75 is the account code FAC, S is the subscriber account code, and N is the destination telephone number.

***75 S N**

Assigning Account Codes

About this task

The messaging software assigns the subscriber's extension as the default account code when no account code is assigned. This default account code is not displayed on the Subscriber screen. Instead, the **Account Code** field on this screen appears blank in this case.

Account codes, other than this default code, can be administered for each subscriber.

To assign account codes to subscribers:

Procedure

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

   The system displays the Manage Subscribers page.
4. Click **Manage** for Local Subscribers or Remote Subscriber depending on the type of subscriber whose extension you want to change.

   The Manage Local Subscribers or Manager Remote Subscribers page is displayed
5. Select the subscriber from the list.
6. Perform one of the following action:
   - Click **Edit/Delete the Selected Subscriber** for local subscribers.
   - Click **Edit the Selected Subscriber** for remote subscribers.
7. Under the **Basic Information** group, in the **Account Code** field, type the account code.

   For new subscribers enter other information as needed. For information on adding a new subscriber, see Adding Subscribers on page 94.
8. Click Save.

Testing the Dialing Sequence

About this task

You can verify the dialing sequence by using the Test Outgoing Call Sequence page. The Test Outgoing Call Sequence page:

- Displays the string of digits that is dialed during an outgoing call.
- Executes the test call by attempting to dial the digits displayed in the **Dialed Digits** field. The system displays information about the dialog that occurred during the test call on the Test Results page

Use this screen to:

- Test a mailbox to determine if an outgoing call placed on behalf of the associated subscriber is being made correctly.
- Test outgoing call functionality in general. For example, you can use the test screen to place an outgoing call to a nearby telephone to verify call completion.
- Account for each digit in the displayed dial string by examining the contents of the **Dialed Digits:** field, for example, the account code feature access code, account code, pauses, and destination number.

To test the dialing sequence:

Procedure

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

   The system displays the Test Outgoing Call Sequence page.
4. Type appropriate values in the field and click **Run Test**.

   Note:

   The test will not run unless the text fields contain the appropriate information.

Result

The system displays the test results.

The system displays the **Dialed Digits** as defined in the **Dialing Sequence** field of the Outgoing Call Sequence page. For example, the **Dialed Digits** field might contain the account code FAC, followed by an account code and a destination number.

Automated Attendants and Bulletin Boards

Overview of Automated Attendants and Bulletin Boards

This section describes how to define and administer automated attendants and bulletin boards with Communication Manager Messaging. The section includes examples you can modify to fit your particular requirements.

This section describes:

- Plan your automated attendant
- Set up an automated attendant, including multilingual and teletypewriter (TTY) greetings
- Set up a business schedule and set up a holiday schedule
- Set up a call routing table
- Plan for your bulletin boards with automated attendant
- Set up a bulletin board

Planning an Automated Attendant

The first step toward setting up an automated attendant or bulletin board is to understand the concepts.

What Is an Automated Attendant?

An automated attendant is an interactive telephone answering system that answers incoming calls with a prerecorded announcement and routes them based on the caller's response to menus and prompts.

You set up an automated attendant so that callers hear a menu of options. Callers then press the button on their telephone keypad that corresponds to the menu option they want. The automated attendant then executes the selected option. Callers who do not have touchtone telephones are typically told that they can hold or call another number to speak with a live attendant.

You can design an automated attendant menu system, or menu tree, to contain subordinate layers of menus or bulletin boards. These submenus, or nested menus, play additional options that can include a choice leading to another nested menu.

The menu options that callers hear are actually personal greetings that you record for the automated attendant's extension. You can easily change the text of the message just as you would any personal greeting. You can also use the Multiple Personal Greetings feature to provide different menus and options for different types of calls.

What Is a Bulletin Board?

A bulletin board is an electronic message system that callers can access to hear messages. Callers dial the bulletin board telephone number and the system answers and presents callers with a recorded message. The major difference between a bulletin board and an automated attendant is that a bulletin board does not have an option to route the call.

Design Considerations

To design your automated attendants to make the most effective use of their capabilities, you must first determine the needs for your business. Will all callers be routed directly to the automated attendant? Will certain options of an automated attendant route callers to other automated attendants? Are there any special needs the automated attendant must address, such as accommodating hearing-impaired callers?

Automated attendant applications can include any of the following:

Main automated attendant	The mailbox where the automated attendant telephone extension connects. The main automated attendant plays a single menu of options for selecting a final destination or presents menu options that differ depending on call types defined with Multiple Personal Greetings, business schedules, or holiday schedules. See Setting Up a Main Attendant on page 185 for more information.
Nested automated attendant	Two or more layers of automated attendants a main automated attendant that contains options leading to one or more secondary (nested) automated attendants that play additional submenus of options. See Setting Up Nested Attendants on page 186 for more information. You must create the nested attendant before you specify it in a main or higher-layer attendant. Create a diagram on paper of the menu tree that you want to use. Then administer the automated attendant system starting from the last (deepest) menu layer and work your way back to the main automated attendant.
TTY (Teletype-writer)	An automated attendant administered with a TDD announcement set that provides service to hearing impaired callers. (The TDD announcement set is recommended but not required to set up TTY automated attendants.) Hearing impaired callers need a

Table continues…

	standard, standalone, acoustically coupled teletypewriter along with a touchtone telephone. See TTY Automated Attendants on page 176 for more information.
Nonresident subscriber extensions	A main automated attendant that contains options leading to subscribers who have voice mailboxes and call in for messages, but do not have actual telephone extensions on the switch. See Setting Up Nonresident Subscriber Extensions on page 187 for more information.
Shared extensions	A main automated attendant that contains options leading to the mailboxes of two or more people sharing the same telephone. See Setting Up Shared Extensions on page 187 for more information.
10 Options per Attendant	The automated attendant can have as many as 10 menu options, corresponding to the buttons 0 through 9 on a touchtone telephone
Automated Attendant Extension on the Switch	If the automated attendant extension is to be called directly, administer the switch to route calls to that extension. You (or the switch administrator) administer the switch to route all incoming calls to an automated attendant instead of to a receptionist, or perhaps to route calls to this extension only after normal business hours. (If the automated attendant is a nested automated attendant, administer the extension as a "phantom" extension.)
COS for Automated Attendants	If you plan to use a number of automated attendants, you might want to set up a class of service (COS) with the **PERMISSIONS, Type:** field already set to **automated attendant**. **Note:** If you set up an automated attendant COs, be sure that existing subscribers are not already assigned to that COS.
*** 8** Transfers	You can administer your system to allow callers to transfer from the automated attendant to a specific extension by entering *** 8**, the extension number, and the pound sign **#.** Generally, it is more efficient to have callers enter extension numbers directly. *** 8** is typically used when the attendant's options require use of all the buttons or when the switch dial plan precludes use of the button that corresponds to the first digit of internal extension numbers that could be called directly. The Call Transfer Out feature must be turned on before callers can use *** 8**. **Security Risk!** Allowing transfers out of the messaging software increases the risk of toll fraud. If you set up your automated attendant to use this feature, be sure you restrict the allowable destination numbers as described under Controlling Call Transfers on page 67.
Direct Transfers without *** 8**	Callers can dial an extension directly from the automated attendant without using *** 8**. To administer such direct dialing, type an **e** in the **Extension** field for the button whose number corresponds with the first digit of real switch extensions (on page

Table continues…

	3 of the Subscriber screen). For example, if internal extensions begin with 5, assign button 5 as extension **e**. This allows the caller to dial any extension that starts with 5. **Note:** For this feature to work properly, **Addressing Format** must be extension on Page 2 of the automated attendant's Subscriber screen. Pay particular attention to the switch dial plan when assigning the **e** option. Some extensions within the group may not exist, may not be assigned, or may be assigned to special features. Any of these situations may cause problems if a caller attempts to dial anything but a voice extension. For more information and instructions, see Step 2: Administering the Automated Attendant as a Subscriber on page 179.
Coverage to Messaging	The automated attendant extension must be administered to cover to the messaging extension with Call Forwarding. Calls are then sent to the automated attendant mailbox where the menu of options is heard.
Call Routing	The messaging software provides a conditional routing capability. You can use a routing table to vary automated attendant operation based on as many as four separate business schedules and as many as four holiday schedules. See Setting Up a Call Routing Table on page 190 for more information. Additionally, a call can be routed to an automated attendant during an alternate time associated with a business schedule, such as lunch time.
Addressing Messages	If you design an automated attendant so callers have the option of leaving messages for multiple messaging subscribers, the messaging feature of addressing messages by name or extension applies. It is a good idea to include this information in the recorded greetings and prompts callers hear.

Modes and schedules

Automated Attendant Modes of Operation

A business can deploy automated attendant service in either primary or secondary operational mode.

Primary Mode Operation

An automated attendant service deployed in primary mode is expected to answer all incoming calls as soon as they come in. The company receptionist backs up the automated attendant by handling overflow calls and calls from people needing assistance, for example, those who press 0 or those who make no selection.

Secondary (Backup) Mode Operation

An automated attendant service deployed in backup mode defers as many calls as possible to the company receptionist. The automated attendant service is configured to back up the company receptionist by handling calls the receptionist is unable to answer.

Operational Schedule

Typically businesses are considered open during the day and closed during the night. The messaging software automated attendant service can be designed to answer incoming calls on a 24-hour/day basis or only at night, depending upon your business needs.

Business Operational Schedule

The automated attendant can use the messaging software weekly business schedule for time-of-day operation or it can rely on the Communication Manager server to indicate when it should operate in a day schedule and night schedule. It makes no difference to the automated attendant service whether day/night operation is controlled by the Communication Manager server or by the messaging software's own weekly business schedule.

Holiday Operational Schedule

The automated attendant can be administered to deviate from the normal business schedule for a day at a time. You might use these schedules to play different greetings and to handle calls differently on holidays. There are four holiday schedules.

Alternate Operational Schedule

The Alternate Service Hours feature allows the automated attendant to play a different menu and/or handle calls slightly differently during lunch time or any other time. The routing table provides a way to do this. This feature can be used independently of the telephone system's night service status.

Routing Table

These operational schedules are tied together within a routing table. A routing table applies the business schedule and a holiday schedule to an incoming called number such as an incoming trunk or covered extension. You then assign a schedule to the automated attendant mailboxes you want to handle the calls at the various times.

See Setting Up a Call Routing Table on page 190 for more information on operational schedules and routing tables.

Using Rotary Telephones with an Automated Attendant

Automated attendants can work with rotary telephone users if the messaging system has an attached pulse-to-tone converter. A pulse-to-tone converter is a box located between the switch and the central office.

To use pulse-to-tone conversion properly, you must allow enough time for the converter to convert the pulse to a tone. Set the **Between Digits at Auto-attendant or Standalone Menu** field on the **System Administration** to between 3 and 12 seconds (5 or 6 seconds is recommended). This value must be sufficient to allow the converter to work. Depending on your system and your converter, it may take actual use to determine the best value.

If a caller fails to enter any tones at an automated attendant menu, the messaging software uses the time-out value administered on the automated attendant's Subscriber screen. This time-out value should be greater than the value of the **Between Digits at Auto-attendant or Standalone Menu**

field on the **System Administration**. If it is not, the automated attendant could time out before the first digit can be entered.

If you are not using a pulse-to-tone converter, leave the **Between Digits at Auto-attendant or Standalone Menu** field on the **System Administration** at the default of 3.

Multilingual Automated Attendants

You can set up a multilingual automated attendant, the first level of which might ask the caller to select a language. Subsequent levels implement the automated attendant in the language chosen.

Multilingual Feature

If you have purchased multiple language announcement sets, the Multilingual feature should be set to ON (check the Feature Options window accessed from Customer/Services Administration on the Main Menu). Your automated attendant can use 2 languages to greet callers during prime and non-prime hours.

The first menu in the automated attendant should be one where the caller chooses a language (such as "Press 1 for English or press 2 for Canadian French"). You can then set up separate menu trees for each language.

For example, your company operates in a U.S. English/Canadian French bilingual environment and uses an automated attendant to redirect calls to the appropriate extension. The following scenario is typical of nested, multilingual automated attendants.

1. The recording for the main or firstlevel automated attendant is in US English (except for the invitation to press 1).
2. "Hello, this is ABC Company."

   "Pour Fran □ s, appuyez sur le un."

   "To talk to a sales agent, please press 2."

   "For billing problems, please press 3."

   "If you know the number of the person you want to reach, please enter it now, or you may wait and an operator will be with you shortly."
3. The caller presses 1. The recording for the secondlevel automated attendant is in Canadian French.
4. (In Canadian French)

   "To talk to a sales agent, please press 2."

   "For billing problems, please press 3."

   "If you know the number of the person you want to reach, please enter it now, or you may wait and an operator will be with you shortly."

   (If the caller presses * 4 for help, Canadian French prompts are used if the primary announcement set is Canadian French.)
5. The caller enters extension number 432.
6. (In Canadian French)

   "Please wait."

7. The call is transferred to extension 432. If the call covers to the messaging software, call treatment in the call answer scenario will be as described above.

To administer an automated attendant to make use of this feature, see Step 2: Administering the Automated Attendant as a Subscriber on page 179.

Multiple Personal Greetings Feature

You can also use the Multiple Personal Greetings feature to customize an automated attendant's spoken personal greeting for calls of various types. This customizing could be cosmetic, such as a formal or informal personal greeting depending on whether the call is external or internal, or it could voice a different set of options, such as offering a restricted menu of choices to out-of-hours callers.

You can set a greeting for different types of calls, for example, internal and external, busy and no answer, and/or out-of-hours. We can record greetings in various languages but can't activate greetings for different languages.

TTY Automated Attendants

To access your automated attendant, hearing impaired callers need a standard standalone, acoustically coupled TTY along with a touchtone telephone. The TDD-English announcement set makes it more convenient to set up teletypewriter (TTY) automated attendants that provide service to hearing impaired callers.

Note:

The TDD announcement set is recommended, but not required, to set up TTY automated attendants.

Planning Your TTY Attendant

The following are recommendations and requirements for planning the use of the TTY automated attendant feature:

- The TDD announcement set should be activated when administering the TTY automated attendant menus. If the TDD announcement set is not running, you must put your ear to the handset resting in the TTY acoustic coupler to hear the spoken messaging announcements that you need to follow while administering the automated attendant menus. Without the TDD announcement set, a hearing impaired person cannot set up automated attendant menus.
- To record automated attendant menus, you need a standalone, acoustically coupled TTY (available from many telephone equipment stores); a TTY with a buffer is recommended since you may want to edit a menu before downloading it to your system. (Refer to the user's guide that came with the TTY for instructions on using your TTY.)
- The TDD announcement set needs to be identified on the Subscriber or Class of Service screen for the automated attendant by setting the **Login Announcement Set** and **Call Answer Primary Annc. Set** fields to **TDD.**
- The use of separate telephone numbers for TTY and voice automated attendants tends to be more user friendly for the intended audiences. While this is not required, it is strongly recommended.
- The Multilingual feature can be used to administer an automated attendant with nested TTY menus and nested voice menus. However, TTY callers see either nothing or only unreadable

characters resulting from voiced prompts or greetings, and hearing callers encounter TTY messaging noise.

- The TTY automated attendant can be administered to use name addressing. The caller must use the touchtone keypad rather than the TTY keyboard to address a message by name.
- TTYs use the Baudot communications protocol in which the same 5bit code can represent either a letter or a nonalphabetic character, such as a number or figure. (For example, the binary code 00001 is both the letter "E" and the number "3".) This sharing of 5bit codes is made possible by having a letters mode and a numbers/figures mode.
- If a TTY receives the 5bit code 11111, it is set to letters mode. The TTY then assumes all subsequent 5bit character codes received are letters. By contrast, if a receiving TTY is set to numbers/figures mode (by receiving the 5bit code 11011), it then assumes all subsequent 5bit character codes received are numbers and figures.

  Important:

  This is important because a TTY that is not in the same mode as the device that is transmitting to it displays characters on the receiving TTY that make no sense to the caller.

  All messaging TTY announcements contain the appropriate mode reset codes to ensure that the receiving TTY stays mode synchronized with your system during announcement playback. It is, however, your responsibility to ensure mode synchronization when recording automated attendant menus.
- Each subscriber or caller who wants to communicate with the TTY automated attendant needs a standard standalone, acoustically coupled TTY and a touchtone telephone. Devices that bypass the touchtone telephone, such as computers with nondialing TTY modems, are unable to issue commands to the messaging software .

TTY Feature Operation

Assign the TTY announcement set on the automated attendant Subscriber or Class of Service screen, and record a TTY automated attendant menu using a TTY (the menu is actually the personal greeting for the automated attendant extension). Instead of speaking the menu greeting into the telephone, type the menu greeting using the TTY keyboard. Callers who reach the TTY automated attendant must use a TTY to interact with the automated attendant.

Here is how a TTY automated attendant relates to other messaging features.

- Automated Attendant: The TTY Automated Attendant feature enables you to set up automated attendants for hearing impaired callers. Any number of subattendants can be administered.
- Multilingual: It is recommended, but not required, that TTY automated attendants have a separate telephone number than voice automated attendants (Call Answer Language Choice set to **n** [no]). Call Answer Language Choice can be set to **y**(yes) to administer an automated attendant with nested TTY menus and nested voice menus. However, TTY callers see either nothing or unreadable characters resulting from voiced prompts or greetings, and hearing callers encounter TTY messaging noise.
- Multiple Personal Greetings: TTY automated attendant menus greetings must be recorded with a TTY. TTY automated attendants may take advantage of the Multiple Personal Greetings feature to record different menus for out of hours and internal and external calls. If the Multilingual feature is on and Call Answer Language Choice is **y** (yes), you record menu greetings using personalized Dual Language Greetings rather than Multiple Personal Greetings.

Mode Synchronization when Recording Menus

Some TTYs have both a letters and a numbers/figures key for switching to the indicated mode. On such devices, if the first character in an automated attendant menu is a letter, press the letters key before you type anything else. If the first character in an automated attendant menu is a number or figure, press the numbers/figures key before you type anything else.

If you do not have these separate keys, synchronization of modes is less convenient, but can be accomplished in the following way:

- If the first character you need to type is a letter, type / (a slash) and press the space bar a few times before you start typing. This causes the system to reset to letters mode.
- If the first character you need to type is a number or figure, type **x** and press the space bar a few times before you start typing. This causes the system to reset to numbers/figures mode.

TTY users need to use both the keypad on their touchtone telephones and the keyboard on the TTY. In menu instructions, make it clear which to use. You might use the word "dial" when the user needs to use the telephone keypad and the word "type" when the user needs to use the TTY keyboard.

When using a TTY to type directly to the system, the messaging software captures and preserves any misspellings, hesitations in typing, and so on. For this reason, it is recommended that you use a TTY with a built-in buffer and completely edit the menu before calling the messaging software to download the buffer. Refer to your TTY user's guide for instructions on editing and downloading the TTY buffer.

Setting Up an Automated Attendant

About this task

Once you design the automated attendant, complete the following steps to set up and check its operation:

Procedure

1. Enable Call Transfers Out of messaging.
2. Administer the Automated Attendant as a Subscriber.
3. Record Greetings for the Automated Attendant Menu.
4. Confirm Automated Attendant Administration.

Step 1: Enabling Call Transfers Out of messaging

About this task

Before an automated attendant can route calls, you must enable the Call Transfer Out feature in the messaging software.

Security alert:

Enabling callers to transfer out of the messaging software has significant security implications. These implications are described under Fraudulent Transfers on page 251. If your system is administered to allow transfer by "digits," ensure that the extension you assign to your automated attendant falls within the range of allowed numbers. See Controlling Call Transfers on page 67 for more information.

To enable call transfers out of messaging:

Procedure

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

   The system displays the Administer System Attributes and Features page.
4. Under the **Call Transfer Out Of Messaging** group, in the **Transfer Type** field, select **Enhanced Cover 0**.

   Enhanced Cover 0 follows the coverage path for the covering extension. Covering extension is the default extension to which a call will be transferred when they press 0 or *0.

Step 2: Administering the Automated Attendant as a Subscriber

About this task

When a subscriber is given auto-attendant permission, that subscriber is added to the attendants list (Under Messaging Administration, select Attendant Management).

For a particular attendant, you can edit settings of this attendant such as, Basic Information, parameters, permissions, incoming mailbox, outgoing mailbox and so on. In addition, you can utilize the special features associated with an automated attendant, such as the actions the automated attendant performs when a caller presses specific buttons. For example, when a caller reaches this auto-attendant, a set of options helps the caller.

You must create a nested attendant before the main or higher-layer attendant that will contain it. See Planning an Automated Attendant on page 170.

For complete information on adding a new subscriber, see the Subscriber Administration section.

Procedure

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

   The system displays the Manage Subscriber page.
4. In the **Local Subscriber** row, click **Manage**.

   The system displays the Manage Local Subscribers page.
5. Select a subscriber from the list and click **Edit/Delete the Selected Subscriber**.

   The system displays the Edit Local Subscriber page.
6. Under the **PERMISSIONS** section, in the **Type** field, select **auto-attendant**.

7. Under the **AUTOMATED ATTENDANT MENU** section, provide appropriate inputs in the fields.
8. Click **Save**.

Automated Attendant Menu field description in the Edit Local Subscriber page

Field Name	Valid Input	Description/Procedure
Allow Call Transfer	yes, no (default)	Allows callers to transfer out of the messaging software with *** 8** when this automated attendant is reached. **Security alert:** To reduce the risk of toll fraud, it is strongly recommended that this field be left at its default setting of n for most attendants.
Button:	Display only	The telephone keypad numbers from 1 to 9 and 0.
Extension:	• 3 to 50 digit extension • e	For each button number you want a caller to use, type a 3-digit to 50-digit extension (depending on your dial plan) or **e**. The default is a blank. • Type an extension if you want to connect a call to this extension when the caller presses the associated button number. The extension could lead to a nested automated attendant or bulletin board, ring at a telephone, or connect directly to a voice mailbox. If the extension leads to a nested attendant, that attendant must already have been created. • Type **e** if you want the caller to dial any extension or name beginning with the associated button number. Callers can dial the extension if the **Addressing Format** field on the Automated Attendant Subscriber page is **extension**.

Table continues…

Field Name	Valid Input	Description/Procedure
		Callers can dial the name if the **Addressing Format** field on the Automated Attendant Subscriber page is **name**. If they are using name addressing, the **Extension** field for buttons 2 through 9 must all be e. The associated voice prompt instructs the caller to enter an extension or name. For a menu with only one button option, the value in this field must be an extension.
Treatment	• Blank • call-answer • guest-greeting • transfer	For any extension listed, enter one of the following to identify how the messaging software handles the call when this button is pressed: • **blank** Means the corresponding button selection on the telephone keypad is not an available menu selection. Note that a blank in the **Extension** field requires a blank in the **Treatment** field. • **call-answer** Puts the call directly into the mailbox for the extension and plays the call answer greeting, attendant menu, or bulletin board message without transferring through the switch. • **guest-greeting** Puts the call into the mailbox for the designated extension (without transferring through the switch), plays the standard guest greeting ("Please leave a message for name"), and allows the caller to record a message. • **transfer** Transfers the call to the extension on the switch.

Table continues…

Field Name	Valid Input	Description/Procedure
Comment	• Blank • From 1 to 29 alpha- numeric characters	This is an optional field that can be used for any notation that could help to identify the extension. This field could be helpful should you need to modify the attendant's functions or re-record the attendant menu at a later date.
Timeout, Extension	• Blank • A 3-digit to 50-digit extension	Specifies the extension to which the caller goes when the timeout period has elapsed. If this field is left blank, the caller is disconnected after two timeout periods elapse.
Timeout, Treatment	• Blank • call-answer • guest-greeting • transfer	See the **Treatment** field description above to determine your choice. This field identifies how the system handles the call if a timeout occurs and no input is received. • If you leave this field blank, the **Timeout, Extension:** field must be blank. • If you type an entry in this field, the **Timeout, Extension:** field must contain an entry.
Timeout, Comment	• Blank • From 1 to 29 alpha- numeric characters	This is an optional field that can be used for any notation that could help to identify the extension. This field could be helpful should you need to modify the attendant's functions or re-record the attendant menu at a later date.
Length of Timeout on Initial Entry:	From 0-9 Default: 5	This is the number of seconds the system waits for a response from the caller.

Step 3: Recording Greetings for the Automated Attendant Menu

Use your touchtone telephone to record the automated attendant menu greetings that callers hear when they press a key on their telephones. You record an attendant menu greeting in the same way you record a personal greeting. The only difference is that you record the greeting for the attendant extension, and the greeting describes the options for the attendant.

It is a good idea to write down a script for the menu greeting ahead of time and read it aloud to a colleague before recording it. We also recommend that you write down the menu greeting numbers so that you have both the number and the corresponding greeting script if you need to re-record any greetings at a later date.

You might want to consider including the following in the menu greeting script:

- A "hello and welcome" greeting followed by the menu choices available to the caller
- An instruction on pressing *** 8** to transfer to a specific extension (if this option is active) and press the pound sign
- An instruction to wait if a time-out extension is administered
- An instruction on pressing *** 4** to repeat the menu selections
- **Note:**

  You can also set up a one-button press to repeat the menu by putting the automated attendant's extension in the **Extension** field and **call-answer** in the **Treatment** field.

Recording an Automated Attendant Menu Greeting (No Multiple Personal Greetings)

About this task

To record a single automated attendant menu greeting (the Multiple Personal Greetings feature is not used):

Procedure

1. Log in as the automated attendant using the extension and password (if any) you assigned on the Subscriber screen.
2. At the activity menu, press **3** to administer the attendant menu.
3. Press **1** to record the attendant menu greeting.
4. Enter a greeting number between 1 to 9.
5. At the tone, speak the scripted greeting for the menu and then press **1** to stop the recording.
   - Press **1** again to record from where you last stopped.
   - Press **2 3** to listen to the recording.
   - Press *** 3** to delete and re-record.
6. Press **#** to approve.

Recording an Automated Attendant Menu Greeting (Multiple Personal Greetings)

With multiple personal greetings, your automated attendant menu greeting can change according to the type of call. For example, you can have one greeting for out-of-hours calls and another for calls during regular business hours. You can also have different menus for internal and external calls.

Note:

If your system should lose any voice messages, for example, due to a disk crash, you must check each of the automated attendant menu greetings to ensure that none were lost. It is a good idea to write down the scripts for the menu greetings as a precaution. If an automated attendant menu greeting is lost, re-record it.

If an automated attendant menu is lost or was never recorded, callers hear a system announcement indicating that attendant services are not available. The system also makes an entry in the

Administrator's Log each time a caller dials the automated attendant extension. You can view these logs at any time (see The Administrator's Log on page 202).

Step 4: Confirming Automated Attendant Administration

About this task

The process of defining an automated attendant menu system is complete when all of its submenus are defined and all the voice prompts including any announcements such as attendant menus are recorded. The Messaging software provides a testing utility. This is a convenient way to test the structure of a menu so that callers do not encounter an incomplete automatic-attendant menu tree.

Procedure

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

   The system displays the Attendants.
4. Select an attendant from the list and click **Menu Tree**.

   The system displays the Auto-Attendant Menu Tree page.
5. In the **Start From Called Party ID in Routing Table** field, select **Yes**.
6. Leave the **Starting Point** field blank to test all mailboxes in the routing table.
7. In the **Report Type (full/errors)** field, select **errors**.
8. Click **Display Menu Tree**.

Result

The program tests all the nested mailboxes. As the testing proceeds, the results displays on the screen.

The testing utility searches automated attendant menus to verify that each mentioned automated attendant mailbox exists and that the necessary personal greeting(s) have been recorded.

Auto-Attendant Menu Tree field descriptions

Field Name	Valid Input	Description/Procedure
Start From Called Party ID in Routing Table?	yes,no	Select **yes** in this field to make the program start its search at the **Incoming Called Number** in the routing table. For the example shown in the Auto-Attendant Routing Table Screen on page 194, if you specified trunk 802 in the next field, then mailboxes 9003, 9004, 9005, and

Table continues…

Field Name	Valid Input	Description/Procedure
		the mailbox in holiday schedule hol1 would all be tested. Select **no** in this field to make the program test the mailbox number specified under **Starting Point** first, and then test the mailboxes that are set out in the menu that applies to the specified mailbox.
Starting Point:	• Blank • From 2 to 10 digits	The extension number of the mailbox or Incoming Called Number that is to be tested. Leave this field blank to test all attendant mailboxes (or all mailboxes in the routing table, if you selected **yes** in the first field).
Report Type (full/errors):	• full,errors	**full** = Display errors and each component element of each mailbox **errors** = Display only flawed mailboxes and errors

Examples of Automated Attendants

The examples in the following topics describe some applications for the Automated Attendant feature. Use these examples as models when defining your own automated attendants.

Setting Up a Main Attendant

A main attendant is an attendant that can be reached directly by callers who dial through your switch. This attendant can answer your company's main telephone, or an individual department's main telephone. It must be associated with an extension that is administered on the switch.

The Edit Local Subsciber page_Automated Attendant section on page 180 example shows the administrative entries for setting up this type of main automated attendant.

For this example, the automated attendant is set up to answer the company's main telephone. It offers callers the option of leaving a message for the sales department; transferring to the accounting, personnel, or payroll departments by pressing a number; dialing any internal extension that begins with 3; or transferring to a receptionist. If the caller does not respond within 5 seconds, the call is transferred automatically to the receptionist.

If the caller chooses to transfer to accounting or personnel, the caller immediately hears the call answer greeting active for the mailbox associated with extension 37200 or 37300. The caller is not transferred through the switch because of the call answer treatment. Finally, to repeat this menu, callers can press `9`.

Switch administration determines when calls are routed to the main attendant's extension. For example, the switch can be administered to route all incoming calls to this extension instead of to a receptionist, or to only route calls to this extension after normal business hours or during busy periods.

Setting Up Nested Attendants

A nested attendant is an attendant that is invoked by another attendant. The nested attendant can also be a main attendant. That is, the extension can be reached directly by internal and external callers who dial the extension number directly.

For example, callers who dial the accounting department's extension directly can hear voice options from a main attendant for that department, as can callers who transfer to the accounting department by pressing 4 at the main menu in the previous example. The accounting department's attendant is said to be nestedbeneath the company's main menu.

Additional menus can be nested beneath the accounting department's attendant, such as for transferring to the payroll or accounts receivable desk.

To administer an automated attendant system that contains nested attendants, you must start from the bottom, or deepest, layer and work your way backwards to the main or higher-layer attendant that will contain it. For instance, to administer the menu system described in the example below, you must define and administer the accounting department automated attendant before defining and administering the main automated attendant.

A good approach to setting up nested automated attendants is to diagram the complete system on paper, including telephone keypad options and their corresponding menu or call treatment. You might also want to write the scripts for the menu greetings at this time. Once you are satisfied with the structure of your menu tree, start administering the tree from the last layer, and continue backwards until you reach and administer the main automated attendant.

A simple example of this application is shown below. In this example, pressing **2** at the main menu transfers the caller to the accounting department's attendant, and pressing **3** at that attendant transfers the call to the payroll department's extension.

Attendant	Button	Extension	Treatment	Result
main	2	52200	call-answer	go to accounting attendant
accounting	3	52205	transfer	transfer to payroll extension

To the caller, this nesting is transparent because the nested attendant is invoked immediately by the system without transferring the caller through the switch. The caller in this example hears the main attendant options, presses **2** to transfer to accounting, hears the accounting department attendant options, and presses **3** to transfer to the payroll extension without the delay that is associated with transferring back through the switch.

Setting Up Shared Extensions

If several subscribers share a single telephone extension, a simple method is required for a caller to leave a message for any of the subscribers or for a specific individual. An automated attendant can handle this task by providing callers with options to leave a message for the extension or any of the individuals who share it. The attendant extension is administered at the switch. Nonresident subscriber extensions in the messaging system, that is, extensions that are not administered at the switch, are used for each of the sharing subscribers. The automated attendant can transfer callers directly to these mailboxes to leave messages.

Note:

Because message waiting indicators (MWIs) are associated with individual telephone sets and not with the messaging software mailboxes, the MWI for a shared extension is be activated when a new message is in the mailbox for the extension number that is shared, but not when new messages are in the mailboxes of the individual subscribers only. If you administer your system to use shared extensions in this way, inform your subscribers to check their mailboxes periodically, whether or not the MWI is active.

For example, a company sets up an information desk with a single telephone to provide callers with any necessary information or assistance. Two people answer the telephone during the day. They do not have individual telephones and can be reached only through the information desk. They are administered as messaging software subscribers and are associated with extensions in the messaging software that are not administered on the switch.

If someone calls the information desk and the telephone is not answered or is busy, the call is routed to the automated attendant. The automated attendant in this example prompts callers to leave a message for the information desk or for one of the individuals who staff the desk.

If the caller selects an individual (button 2 or 3 in this example), the caller goes directly to the subscriber's messaging mailbox to hear the individual's call answer greeting and then leaves a message. If the caller does not respond to the automated attendant prompt within 5 seconds, the messaging software plays the system guest password greeting, "Please leave a message for <name>." The voiced name in this example is whatever name is recorded for the subscriber with extension 37001. This name is probably "information desk," since that is the name of the extension.

In this example, a message left in the mailbox of the information desk extension activates the extension's message waiting indicator (MWI). A message left in the mailbox of one of the sharing individuals does not. These individuals must call into the messaging software to check for messages or use the Outcalling feature.

Setting Up Nonresident Subscriber Extensions

Nonresident subscribers are messaging software subscribers who do not have an extension on a switch that is served by the messaging software. Mailbox numbers in the system for these subscribers correspond to the messaging software extensions that are not administered on the switch. (The subscribers with extensions 33304 and 33305 in the previous example are nonresident subscribers.)

Security alert:

Setting up nonresident subscribers with numbers that begin with trunk dial access codes could contribute to toll fraud. Always assign extensions that do not allow access to any outside lines. For more information about guarding your system against toll fraud, see System Security on page 251.

An example of a nonresident subscriber is an outside sales representative who needs to receive messages from clients. To accommodate this type of subscriber, an automated attendant can be set up to move callers directly to nonresident subscriber mailboxes. The caller needs to know only the number of the automated attendant and the nonresident subscriber's mailbox number to leave a message. Once in the nonresident subscriber's mailbox, the caller hears either the system guest greeting or the nonresident subscriber's call answer greeting, depending on the transfer treatment that is specified on the Subscriber screen.

In this example, the extension number for each nonresident subscriber is a 5-digit number beginning with 3, and the extension number for the automated attendant is 37001. The nonresident subscriber provides clients with the telephone number of the automated attendant and the subscriber's own mailbox number.

With the system administered in this way, clients dial xx3-7001, listen to the automated attendant menu, enter the nonresident subscriber's mailbox number, listen to the subscriber's personal greeting, and leave a message. If the caller does not enter a mailbox number within 5 seconds, the call is transferred to a sales clerk.

If the treatment for calls that go directly to mailboxes is "guest-greeting" instead of "call-answer," callers hear the system guest greeting "Please leave a message for name" instead of the nonresident subscriber's personal greeting.

Setting Up Automated Attendants to Transfer by Name

Automated attendants can allow callers to transfer to subscribers by spelling out subscriber names.

Follow the procedure below to preform the transfers by name:

- Enter **name** in the **Addressing Format** field on page 2 of the Subscriber screen.
- Set buttons 2 through 9 to **e** on Automate Attendant Menu section of the Edit Local Subscriber page as described in the Edit Local Subsciber page_Automated Attendant section on page 180 table.

The voiced menu for this type of automated attendant should tell the caller to spell the person's name to which they want to transfer, last name first, by pressing the keys on the telephone keypad. Because callers use only the numbers 2 through 9 to spell a name, you can code buttons 1 and 0 to transfer directly to another destination (such as a live attendant). In this case, the menu should also instruct callers on how to transfer by extension (for example, "To transfer to an extension, press star 8 (*T) and the 5-digit extension number, followed by the pound sign.").

Using Multiple Greetings for Automated Attendants

The Automated Attendant feature can be quite flexible when used with the Multiple Personal Greetings feature. Since the voiced menu is the personal greeting for the automated attendant's

extension, administering personal greetings for an automated attendant is the same as for any subscriber.

The Multiple Personal Greetings feature allows you to specify as many as 9 unique personal greetings for the extension, and to specify circumstances for using different greetings, such as for internal and external calls, busy and no-answer calls, and out-of-hours calls. Use the System Administration screen to define the out-of-hours period. Calls made outside of prime time as defined on that screen are considered to be out-of-hours.

If an out-of-hours greeting is selected, it overrides internal/external and busy/no-answer identification for all calls received during the period designated out-of-hours. Note that multiple greetings can be set up for either internal/ external or busy/no-answer, but not for both at the same time. Internal/external and out-of-hours make sense for most automated attendants.

When used for an automated attendant, multiple personal greetings allow you to provide not only different greetings, but to voice different options for selected types of callers. Even though the voiced greetings are different for different types of callers, the available menu options remain the same for each call.

For example, you can define the following greetings for the automated attendant:

1. For all external calls, the greeting is:
   - "Thank you for calling Smith and Jones."
   - "To transfer to a specific extension, enter that extension now."
   - "To reach the sales department, press 1."
   - "To reach the accounting department, press 2."
   - "To reach the personnel department, press 3."
   - "To get further assistance, press 0 or wait."
   - **Note:**

     You may want to have a main automated attendant that has a greeting similar to, "Thank you for calling Smith and Jones. If you have a touchtone telephone, press 1. If you are calling from a rotary telephone, please wait and an attendant will be with you shortly."
2. For all internal calls, the greeting is:
   - "To reach a specific person, enter the extension."
   - "To reach Sales, press 1."
   - "For Accounting, press 2."
   - "For Personnel, press 3."
   - "For Security, press 8."
   - "To access employee bulletin board information, press 9."
3. For all out-of-hours callers, the greeting is:
   - "Thank you for calling Smith and Jones."

- "Our normal office hours are 8 a.m. to 5 p.m. Monday through Friday."
- "To leave a message for a specific person, enter the mailbox number using the keys on your touchtone telephone."
- "If this is an emergency, please press 8."

The example above allows the automated attendant to voice specific information for different types of callers and to exclude or include options depending on caller type.

Note:

All options listed on the Subscriber screen are available to all callers; they are just not mentioned as options in the greeting.

Setting Up a Call Routing Table

The messaging software provides a conditional routing capability. You can use the routing table and its associated screens to base automated attendant operation on as many as 4 business schedules and as many as 4 holiday schedules.

Overview of Business Schedules

The business schedules divides the 24-hour day into three parts called day service, night service, and alternate service.

Day and Night Service

Calls can be routed to one mailbox for day service and to another for night service. A business may, for example, set day-service hours to be the period when the business is open, and it may send calls to a night-service mailbox during the remaining hours and on weekends.

Since 4 business schedules are available to you, you can use both arrangements as necessary for differing purposes.

Alternate Service

Alternate service is a period of time that you can define when calls may be sent to a third destination during either day- or night-service hours. This period may be used, for example, to provide a special automated attendant to handle calls from other time zones during the transition from day to night service. Alternate service can also be used to cover for an operator during the lunch hour.

Overview of Holiday Schedules

Holiday schedules make it possible to deviate from the normal business schedule for a day at a time. You might use these schedules to play different greetings and to handle calls differently on holidays. There are four holiday schedules. On each of them, you can record up to 26 dates along with the automated attendant mailbox to be used on each date. If you have separate schedules for the sales office and for the warehouse, for example, you could send sales-office calls to one mailbox during a sales conference, and warehouse calls to another mailbox during inventory time.

Overview of the Routing Table

The business and holiday schedules are tied together within a routing table. A routing table applies the schedules to an incoming called number such as an incoming trunk or covered extension. You administer the routing table so that the automated attendant extension you want to handle the calls at the various times is also tied with the appropriate schedule.

When a caller dials a number that appears in the left most column of the routing table, the holiday schedule is checked first. If the current date does not appear in the holiday schedule, the business schedule is checked. If the time of day is covered in the business schedule under alternate service, the call is sent to the alternate service mailbox. If not, then depending on the time of day, the call is sent to the day-service or to the night-service mailbox.

Setting Up a Business Schedule

About this task

See Overview of Business Schedules on page 190 for a detailed description of the process for setting up a business schedule.

To set up the business schedules:

Procedure

1. Open a Web browser and in the Address field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the left hand pane, under the **Messaging Administration**, click **Attendant Management**.
4. Select an attendant from the list and click **List Schedules**.

   The system displays the list of the business and holiday schedules for the selected attendant.
5. From the **Business Schedules** box, select the **bus1**.
6. Click **Edit the Selected Schedule**.

   The system displays the Auto-Attendant Routing Business Schedules page.
7. Provide appropriate inputs in the fields and click **Update** to save the changes.

Auto-Attendant Routing Business Schedules field descriptions

Field Name	Valid Input	Description/Procedure
Business Schedule	From 1 to 8 alphanumeric characters Default: bus#	OPTIONAL: Type a new schedule name if the default name for the schedule does not seem descriptive enough.
Days of Week	Display only	Starting with Monday, the weekdays are listed in this display-only column.
Day Service Hours	24-hour clock time in the format hh:mm	In Day Service Hours AM starts at 00:00, midnight. PM times are from 12:00 to 23:59. Hours outside of this range are considered to be night service hours.
Day Service Hours > **Start Time**		Type in the time at which daytime operation of a telephone has to begin in the **Start Time:** field.

Table continues…

Field Name	Valid Input	Description/Procedure
Day Service Hours > **End Time**		Type in the time at which daytime operation of a telephone has to end in the **End Time:** field.
Alternate Service Hours	24-hour clock time in the format hh:mm	In Alternate Service Hours AM starts at 00:00, midnight. PM times are from 12:00 to 23:59. Alternate service hours indicates times that can be considered an exception to normal day service (lunch time, for example). An alternate service period must either fall entirely inside or entirely outside of day service hours.
Alternate Service Hours > **Start Time**		Type in the time at which alternate service has to begin in the **Start Time:** field.
Alternate Service Hours > **End Time**		Type in the time at which alternate service has to end in the **End Time:** field.

Setting Up a Holiday Schedule

About this task

See Overview of Holiday Schedules on page 170 for a detailed description of the process for setting up a holiday schedule.

To set up the holiday schedule:

Procedure

1. Open a Web browser and in the Address field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the left hand pane, under the **Messaging Administration**, click **Attendant Management**.
4. Select an attendant from the list and click **List Schedules**.

   The system displays the list of the business and holiday schedules for the selected attendant.
5. From the **Holiday Schedules** box, select **hol1**.
6. Click **Edit the Selected Schedule**.

   The system displays the Auto-Attendant Routing Holiday Schedules page.

   Note:

   The automated attendant must be set up before you can type it in the **Mailbox** field.
7. Provide appropriate inputs in the fields and click **Update** to save the changes.

Auto-Attendant Routing Holiday Schedules field descriptions

Field Name	Valid Input	Description/Procedure
Holiday Schedule	From 1 to 8 alphanumeric characters	Type a new schedule name, if the default name does not seem descriptive enough.
Holiday Name	From 1 to 18 alphanumeric characters	OPTIONAL: The name of the holiday. This field is for your convenience and is not used by the system.
Date	Month and day in the format mm/dd	The date the system forwards the affected incoming call to a mailbox.
Mailbox	Any existing mailbox extension	OPTIONAL: The mailbox extension of the automated attendant to be used for this holiday. This can be a specific reference or a general one. For example, you can make separate extensions for such holidays as New Year's Day and Independence Day, or you can route to one extension for all holidays. If you choose separate extensions, be sure to record each greeting as described in Step 3: Recording Greetings for the Automated Attendant Menu on page 182. Holidays with no mailbox extension are ignored by the call routing function.

Button	Description
Update	Updates the Auto-Attendant Routing Holiday Schedules page.
Back	Navigates to the last page that you visited.

Completing the Routing Table

About this task

Use the Auto-Attendant Routing Table page to configure auto-attendant routing based on holidays and time of day.

The routing function redirects calls to specified numbers according to the instructions given in the business and holiday schedules and the routing table.

To complete the routing table:

Procedure

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

   The system displays the Attendants page.
4. On the Attendants page, click **Routing Table**.
5. Provide appropriate inputs in the fields and click **Update** to save the changes.

Auto-Attendant Routing Table field descriptions

Field Name	Valid Input	Description/Procedure
Incoming Called Number	From 1 to 8 alphanumeric characters	The numbers to be redirected. These can be any incoming numbers reported to the messaging software by the switch, for example, perhaps an incoming trunk number or an extension number that the caller dialed. If a number appears twice in this column, the first instance prevails. For example, 802 appears before the range 802806, and is treated separately per its first appearance. However, 805 appears after the range of numbers, so it is treated as set out on the line associated with the range, and ignored.
Business Schedule	• From 1 to 8 alphanumeric characters • From 1 to 4	The name or number of the business schedule that determines how the incoming number is treated. The name loginis reserved to indicate that a direct, external call to the associated incoming number is allowed to log in; that is, if you call in over this trunk, the messaging software asks you to log in.
Holiday Schedule	• 1- to 8- alphanumeric characters • 1-4	The name or number of the holiday schedule (if any) that determines how the incoming number is treated on holidays.
Day Service Mailbox	An existing mailbox extension	All automated attendant mailbox extensions must be defined before they can be entered in these columns. Type the extension number of the automated attendant mailbox to be accessed during the business hours given in the business schedule. This field must be filled in if the associated business schedule specifies day service hours.
Night Service Mailbox	An existing mailbox extension	Type the extension number of the automated attendant mailbox to be

Table continues…

Field Name	Valid Input	Description/Procedure
		accessed during the period not otherwise specified in the business schedule.
Alternate Service Mailbox	An existing mailbox extension	The extension number of the automated attendant mailbox to be accessed during the alternate-service period given in the business schedule. This field must be filled in if the associated business schedule specifies alternate service hours.

Viewing a List of Automated Attendants

About this task

The List Attendants screen lists the automated attendants by their extension numbers. The list is in numerical order of extension number starting with either the lowest extension number or the extension specified in the command line.

To view a list of automated attendants:

Procedure

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

   The system displays the Attendants page.
4. To view all the attendants, click **List Attendants**.

   The system displays the Attendants page and list of the configured Automated Attendants.
5. In the **List attendants starting with this extension** field, type an extension number of attendants you want to view.
6. Click **List Attendants**.

   The system displays the specified attendant if configured previously.

Viewing a List of Automated Attendant Schedules

About this task

The Auto-Attendant Schedules screen lists the automated attendant holiday schedules and business schedules by name and number. The list is in numerical order by schedule number.

To view a list of automated attendant schedules:

Procedure

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

   The system shows the Attendants page.
4. Click **List Schedules**.

   The system displays a listing of the names and numbers of all business and holiday automated attendant schedules.
5. Click **Back** to return to the previous menu.

Setting Up a Bulletin Board

A bulletin board is an electronic message system that callers can access to hear messages. Callers dial the bulletin board telephone number or reach it via an automated attendant, and the system answers and presents callers with a recorded message. The major differences between a bulletin board and an automated attendant are as follows:

- A bulletin board does not have an option to route the call.
- A bulletin board does not present a menu of buttons for callers to select.
- A bulletin board does not have the capability to allow callers to replay the greeting.

This extension is administered on the switch to immediately forward calls to the messaging software. The message that callers hear is the personal greeting for the bulletin board's mailbox.

Bulletin boards are administered as regular subscribers, with some exceptions, such as typing **bulletin-board** in the **PERMISSIONS, Type:** field of the Subscriber screen.

Note:

The messaging software does not disconnect the call after a caller listens to a bulletin board greeting. In the bulletin board greeting, you should instruct listeners to hang up after listening to the message.

Completing the Subscriber Screen

About this task

See the Subscriber Administration on page 91 section for tasks and field descriptions on adding a new subscriber.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.

3. In the left navigation pane, under the **Messaging Administration** group, click **Subscriber Management**.
4. In the **Local Subscriber** row, click **Manage**.

   The system displays the Manage Local Subscribers page.
5. Select a subscriber from the list and click **Edit/Delete the Selected Subscriber**.

   The system displays the Edit Local Subscriber page.
6. Under the **PERMISSIONS** section, in the **Type** field, select **bulletin-board**.
7. Click **Save**.

Recording the Bulletin Board Message

About this task

You record a bulletin board message in the same way you record a personal greeting. It is a good idea to write down a script for the bulletin board ahead of time and read it aloud to a colleague before recording it.

Note:

The messaging software does not disconnect the call after a caller listens to a bulletin board greeting. Therefore, you should instruct listeners to hang up after listening to the message.

To record the bulletin board message:

Procedure

1. Using your touchtone telephone, call the messaging software and log in using the extension and password of the bulletin board.
2. At the activity menu, press **3** to record the message.
3. Press **1** to record the bulletin board greetings.
4. Press a numbered button to specify the greeting number.
5. At the tone, speak the scripted greeting for the menu and then press **1** to stop the recording.
   - Press **1** again to record from where you last stopped.
   - Press **2 3** if you want to listen to the recording.
   - Press *** 3** if you want to delete and re-record.
6. Press **#** to approve.
7. Press **1** to activate the recording for all calls.

Result

With multiple personal greetings, your bulletin board message can change according to call type(s) (for example, use one message for internal calls and another message for external calls).

Using Bulletin Boards with an Automated Attendant

An automated attendant may present multiple choices for listening to bulletin board messages that are set up with the information service Bulletin Board feature. Use the call answer treatment on the screen for bulletin board extensions to route callers directly into the selected bulletin board's mailbox.

For example, you could set up three different bulletin boards, then set up an automated attendant.

In this example, the automated attendant would prompt the caller to press the appropriate button to hear a bulletin board message. You can use ***8** to transfer call from both bulletin board and auto attendant using bulletin board.

Bulletin board extensions in this example are messaging extensions that are not administered at the switch. These extensions can only be reached by dialing this automated attendant. Callers who select one of these extensions are forwarded directly to the extension's mailbox to hear the call answer greeting.

Audits

Voice messaging database audit overview

During normal operation, the messaging databases work independently under the direction of a set of software managers. These managers, in tandem with hardware and firmware managers, allow the files, databases, and system hardware to work together.

Because databases are handled separately, different databases can contain conflicting information. For example, if a subscriber is removed from the messaging system, other databases may contain messages addressed to that subscriber. In addition, mailing lists that include the deleted subscriber's name can still exist.

To reconcile possible conflicts among databases, software programs called audits run automatically to check for inconsistencies. You can also run audits on demand.

Voice messaging database audit types

The Voice Messaging Database Audits table shown below lists the types of voice messaging database audits.

Table 10: Voice Messaging Database Audits

Audit	Function	Frequency
Mailboxes	Checks and deletes new, old, and unopened messages that exceed maximum retention time	Daily
Clears new, old, and unopened broadcast-deleted messages from subscriber mailboxes	Daily	

Table continues…

Audit	Function	Frequency
Verifies that the Messaging MWL status matches with the switch's MWL status for each subscriber	Daily	
Checks for valid mailbox structure	Weekly	
Makes space-accounting corrections on a per-subscriber and system basis	Daily	
Checks for valid message subscriber IDs	Weekly	
Mailing Lists	Counts subscriber lists and entries on a system and per-subscriber basis to ensure that they are not exceeding internal limits	Weekly
Removes deleted subscribers from lists	Daily	
Removes deleted remote subscribers from local mailing lists	Daily	
Audits delivery manager queues and makes undeliverable entries for deleted subscribers	Daily	
Names	Matches each voice name with a valid local or remote subscriber	Weekly
Logs messages in the administrator's log for the first 20 local subscribers who do not have voiced names	Weekly	
Network Data	Deletes subscribers on remote nodes that have been eliminated from the network	Weekly
Compares internal network files to synchronize information on nodes and subscribers, for example, which node each subscriber belongs to	Weekly	
Personal Directories	Removes deleted subscribers (local and remote) from local subscribers' personal directories	Daily
Subscriber Data	Checks delivery lists associated with current outgoing messages	Daily
Validates fields in class of service templates, subscriber profiles, and automated attendant profiles	Weekly	

Table continues…

Audit	Function	Frequency
Counts subscribers to ensure that the number of subscribers is not exceeding internal limits	Weekly	
Checks the system guest password against individual subscriber passwords and makes appropriate entries in the administration log	Weekly	
Checks subscriber profiles against class of service templates and changes subscribers to class of service	Weekly	
Deletes remote unverified subscribers who have not been on delivery lists in the last 24 hours	Daily	
Deletes remote subscribers with no valid nodes	Weekly	
Deletes unadministered remote subscribers who have not used the system for a specified time period	Daily	
Cross-checks name, extension, touchtone, subscriber directory, and remote node list translations files for consistency with subscriber profiles	Weekly	

Performing a voice messaging database audit

About this task

All voice messaging database audit types use the same general procedure.

Procedure

1. Log in to the Communication Manager Messaging web page.
2. Under Utilities, select Messaging DB Audits.

   The system displays the Audits page.
3. Click the appropriate link for the audit.

To Audit	Click
View Audit History	**History**
Mailboxes	**Start Mailboxes Audit (Mailboxes, Mailbox Data)**

Table continues…

To Audit	Click
Mailing lists	**Start Mailing Lists Audit (Mail Lists, Delivery Data)**
Names	**Start Voice Names Audit (Voice Names)**
Network data	**Start Network Data Audit (Machine Translations, Network Translations, Network Data)** **Note:** This audit is available only if the system has Digital Networking.
Personal directories	**Start Personal Directory Data (Personal Directories)**
Subscriber data	**Start Subscriber Data Audit (Subscribers, Delivery Data)**
Nightly Audit	**Start Subscriber Data Audit (Subscribers, Delivery Data)**
Weekly Audit	**Start Weekly Audit (Weekly, Delivery Data, Network Data, Mailbox Data)**

The system displays the audit name and Result code, which indicate that the audit is running. The system also displays results of in stages depending on how the feature has been designed.

4. Wait for the audit to finish.
5. If the audit fails, perform the following steps:
   a. Resolve any active alarms and rerun the audit.
   b. If the audit fails again, contact the remote service center.
   c. If the system is not providing service and the remote service center cannot help immediately, stop messaging and reboot the system.

Reports overview

Communication Manager Messaging collects information that depicts how the system is used, including data about features, subscribers, communities, data port loads, and remote messaging traffic. This information is displayed in real-time dynamic report windows, in alarm logs and administrator's logs, and in messaging traffic reports.

Alarm logs and administrator's logs record events that are useful for preventive maintenance, for diagnosing problems and troubleshooting the system, and for spotting trends or estimating future needs. Dynamic windows allow you to watch real-time traffic in the messaging system. The table for Traffic Reports on page 263 contains a list of available reports.

The procedures in this topic assume that you know basic messaging commands and navigation, such as logging in and out of the system, command prompt function and usage, and moving from

field to field within a screen or window. If you are not familiar with messaging system basics, read the Management tools section.

Administrator's log

About this task

Access the Administrator's Log to view current error messages and a description for each problem.

The Administrator's Log identifies system events. These events include problems that you need to correct. Some events, such as full subscriber mailboxes and undeliverable messages, directly affect message processing.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Logs** section, click **Administrator**.

   The system displays the Administrator's Log page.
4. Provide appropriate information to run the report.
5. Click **Display**.

   When the system gathers the information you specified, it displays the report results.
6. Examine the displayed events.

   Events, alarms, and their associated repair procedures are described in the *Communication Manager Messaging Alarms and Maintenance Guide*.
7. If a displayed event calls for repair, take whatever corrective action is necessary.

Administrator's log field descriptions

Name	Description
Start Date	The beginning date for the log report in the format mm/dd/yy. If you leave this field blank, all qualifying alarms are displayed. The default value is the current date.
Time	The beginning hour and minute that the report begins. The time is displayed as a 24-hour clock time in the format hh:mm:ss. The **Start Date** field must have valid entries before you can use this field. If the **Time** field is blank, all alarms for the specified start date are displayed. The default value is the beginning of the day 00:00:00.
Application	The two-character code that identifies each module in the system: EL = Enhanced-List Application IM = Internet Messaging LD = LDAP

Table continues…

Name	Description
	MT = Maintenance SM = Station Manager VM = Messaging (voice mail, fax mail, and email messages) VP = Voice Platform You can also select ALL to display the appropriate entries for all applications.
Event ID	The event ID for a specific event. The event ID can contain 1 to 14 alphanumeric characters. A blank field displays all event types. See *Communication Manager Messaging Alarms and Events Guide* for a list of valid administration event IDs.
Search String	A text string that you want the system to search for in the administrator's log entries. The system searches the **Message** field of the administrator's log for matching text. This field can contains from 1 to 78 characters.

Administrator's Log results field descriptions

Field	Description
Date	The dates that the alarms were logged.
Time	The times on the given dates that the administration alarms were logged.
App	The two-character code that identifies each module in the system: EL = Enhanced-List Application IM = Internet Messaging LD = LDAP MT = Maintenance SM = Station Manager VM = Messaging (voice mail, fax mail, and email messages) VP = Voice Platform
Event ID	The code for the administration event type.
Cnt	The number of times that the associated message was sent to the administrator's log within 1 minute.
Message	A textual description of the administration event. Two lines are used for each event.

Activity log

The Activity Log is an administrative tool useful for investigating reported problems with message delivery and the operation of the message-waiting indicator (MWI). The Activity Log maintains a history of the activity on the messaging system. You can use this log to track a specific subscriber's activity by extension and time, and you can often resolve reported problems by observing the Activity Log before filing a trouble report.

Setting activity log data collection options

About this task

Use the Activity Log screen to set up the Activity Log. You can set the following log options:

- Enable or disable the Activity Log.
- Instruct the Activity Log to record MWI updates.
- Set a maximum number of Activity Log entries.
- Clear all entries in the Activity Log.

Note:

If you set the Activity Log to record MWI updates, the number of records that are generated then increase significantly and could create an unduly long log. It is recommended that this field is only enabled when necessary.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Messaging Administration** section, click **Activity Log Configuration**.
4. Provide appropriate information to configure the subscriber activity log, and click **Save**.

Configure Subscriber Activity log field descriptions

Field Name	Description
Activity Log Enabled?	Activates data collection for the activity log. The valid inputs for this field are: yes (default) no
Record MWI Updates?	Activates the recording of message-waiting indicator (MWI) updates that are sent from the messaging system to the switch. The valid inputs for this field are: yes (default) no MWI update records are written to the activity log file only if both the Activity Log feature and the recording of MWI updates are enabled. **Note:** Enabling this feature increases the number of records written to the activity log.

Table continues…

Field Name	Description
Maximum Number of Activated Log Entries	The maximum number of records in the activity log file. This value can range from 1 to 9999999. The default value is 9999999. **Note:** The system clears the log if this number is less than the number of records currently in the log. The system prompts you to confirm this action before continuing.
Clear All Entries in Activity Log	Resets the entries in the activity log. The valid inputs for this field are: yes no (default)

Understanding Log Entries

The Activity Log shows activity information for a selected subscriber. Events are listed in chronological order (oldest first) beginning with the specified date and time. Before running this report, you must first instruct the system to collect activity data.

Received entries

A received entry is made in the Activity Log each time a message is delivered to a subscriber's mailbox. Note that a message with multiple recipients generates a received entry for each recipient. The message can be one of the following:

- Voice mail (VM)
- Priority voice mail
- Call Answer (CA)
- Leave Word Calling (LWC)
- Undeliverable message notification

Scheduled entries

A scheduled entry is made in the Activity Log each time that a message is scheduled for delivery. Only one scheduled entry is made for a message regardless of the number of recipients. The message can be one of the following:

- Voice mail
- Priority voice mail
- Call Answer

Since CA messages are scheduled for immediate delivery at the time that they are created, the scheduled delivery time is not repeated on the display. In addition:

- If both the calling party and the called party are local subscribers, the display shows that the calling party scheduled the message for the called party.
- If the calling party is not a local subscriber, the activity is not recorded.

- If the called party is not a local subscriber, the local messaging system has no knowledge of the call, and the activity is not recorded.

Running an activity log report

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Logs** section, click **Subscriber Activity**.

   The system displays the Subscriber Activity Log page.
4. In the **Mailbox Number** field, type the mailbox number for the subscriber whose activity log you want to display.

   The **Mailbox Number** field takes extensions in the 3-digit to 50-digit range.
5. Select the duration from the **Start Date** and **End Date** fields for which you want to view the subscribers activity.
6. Click **Display**.

   Note:

   This report can take several minutes to run depending on the system load and the size of the log file.

Subscriber Activity Log field descriptions

Name	Description
Mailbox Number	The subscriber telephone extension that you entered on the command line when you generated the report.
Name	The subscriber name that corresponds to the extension that you entered on the command line when you generated the report.
SELECTION CRITERIA	
Start Date	The calendar date at which the report begins. If you leave this field blank, the earliest available date for this subscriber displays.
Start Time	The 24-hour time at which the report begins. If you did not specify a starting date, you must leave this field blank.
End Date	The calendar date at which the report ends. If you leave this field blank, you must also leave the time field blank.
End Time	The 24-hour time at which the report ends. If you did not specify a starting date, you must leave this field blank.

Displaying the alarm report

About this task

The alarm report lists active or resolved messaging system alarms. The most severe alarms are always listed first since these are most often the cause of the problem.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Logs** section, click **Alarm**.

   The system displays the Alarm Log page.
4. Enter values on this page that specify the type of alarm information you want the system to gather.

   The default values of these fields are as follows:

   - Alarm type: Active
   - Alarm level Major?: yes, Minor?: yes, Warning?: yes
   - Start Date: the current date
   - Time: 00:00:00
   - Application: All
   - Resource Type: blank
   - Alarm Code: blank
5. To start the report, click **Display**.

   When the system gathers the information you specified, it displays the Alarm Log page.

Alarm log field descriptions

Name	Description
Alarm Type	The selected alarm type in the report. The valid inputs are: active resolved
Alarm Level, Major?, Minor?, Warning?	Select **yes** to display the alarm level or **no** to omit that alarm level from the report. You can request major alarms, minor alarms, warnings, or any combination thereof.

Table continues…

Name	Description
Start Date	The date from which the alarm report begins. If you leave this field blank, the system displays all recorded alarms of the type specified in the **Alarm Type** field.
Time	The hour, minute and second that you want the alarm report to begin. The **Start Date** field must have a valid entry before you can enter the time. If you leave this field blank, the system displays all alarms for the specified start date.
Application	The two-character code that identifies each module in the system: EL = Enhanced-List Application IM = Internet Messaging LD = LDAP MT = Maintenance SM = Station Manager VM = Messaging (voice mail, fax mail, and email messages) VP = Voice Platform You can also select ALL to display the appropriate entries for all applications.
Resource Type	A specific type of alarmed resource for the alarm report, such as alarm_orig, mirror, netwk_bd. If this field contains a resource type, only alarms related to the specified resource type are displayed. If you leave this field blank, all resource types are included in the report. **Note:** If you use a specific resource type, note the alarm code that is listed with it. You will also need to enter that information on this page.
Alarm Code	The alarm code that corresponds to the resource type. If you did not enter a resource type, you can enter an alarm code. In this case, the report will contain multiple resource types with the same alarm code.

Alarm Log report results field descriptions

Name	Description
App	The code for the application that generated the alarm (active or resolved.)
Resource Type	The specific type of alarmed resource you requested when generating the report, or all resource types if you did not specify a resource type.
Location	A six-character location for the corresponding fault resource type.
Alarm Code	The specific alarm code that you requested when generating the report, or all alarm codes if you did not specify a resource type.
Alm Lvl	The alarm severity level, that is, MAJ(major), MIN(minor), or WRN(warning).
Ack	y = alarm was present during the last referral call. (The alarm was reported to the services organization.) However, alarms might not have been reported if there was a significant number of higher priority alarms.

Table continues…

Name	Description
	n = alarm was not present during the last referral call.
Date/Time Alarmed	The date (month, day, and year) and the time (hour and minute) at which the alarm was raised against the given resource. If these fields are blank, the alarm is currently active. These fields must always have a value.
Date/Time Resolved	The date (month, day, and year) and the time (hour and minute) at which the alarm was resolved. If these fields are blank, the alarm is currently active. If only active alarms are displayed, these fields must always be blank. If only resolved alarms are displayed, these fields must always have a value.
Resolve Reason	The cause of the alarm resolution. There will be a value in this field only if you choose to report on resolved alarms. The resolution values are: • Maint: The alarm was resolved by maintenance and the resource recovered. • Reboot: The system was rebooted, and all active alarms are resolved. • Remove: The alarm was resolved by removing the resource. If this field is blank, the alarm is currently active.

Communication Manager server view current alarms page

The Communication Manager server view current alarms page lists outstanding alarms against the Communication Manager server, and messaging software. This screen shows either:

- A summary of alarms, if present, followed by detailed table of explanation, or
- A message stating that no alarms are present.

Communication Manager must be running to view alarms using this screen. If Communication Manager is not up, the system displays a message indicating that an error occurred while retrieving server alarms.

Viewing current alarms

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the **Alarms** section, click **Current Alarms**.

   The system displays the Current Alarms screen.
4. Check whether any alarms are present under the **Messaging Alarms** section.

Viewing the administrator's history log

About this task

The Administrator's history log identifies administrative events that occur on your system. These events include information about any changes to your system, such as logins, command line entries, reports that were run, or changes to software.

To view administrative events that occur on your system:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Logs** section, click **Administration History**.

   The system displays the Administration History Log page.
4. Enter appropriate values in the **Start Date**, **Time**, **Application**, and **Search String** fields.
5. Click **Display** to start the report.

   When the system gathers the information you specified, it displays the report in the report results.

Administration history log field descriptions

Name	Description
Start Date	The beginning date for the log report. The default value is the current date.
Time	The beginning hour, minute and second that the report begins. The **Start Date** field must have valid entries before you can use this field. The default value is the beginning of the day 00:00:00.
Application	The two-character code that identifies each module in the system: EL = Enhanced-List Application IM = Internet Messaging LD = LDAP MT = Maintenance SM = Station Manager VM = Messaging (voice mail, fax mail, and email messages) VP = Voice Platform You can also select ALL to display the appropriate entries for all applications.
Search String	A text string that you want the system to search for in the administrator's log entries. The system searches the **Text** field of the administrator's history log for matching text. The search string can contain 1 to 78 characters.

Administration history log report field descriptions

Name	Description/Procedure
Date/Time Rec	The date and time that the event occurred, in mm/dd/yy hh:mm:ss format.
App	The abbreviation for the application that was affected by the event.
Event ID	Always displayed as ADMIN001.
Cnt	The number of times that the exact message was received within one second.
Message	This field is not labeled, but it is the last field in each event entry. The text field shows the exact command that was given to the system. The command information is enclosed in single quotation marks, such as 'command information'. The command could have been provided by any of the following: • AKS = An application external to messaging that performs administrative updating or reporting tasks • API = An application external to messaging that interfaces with the messaging software through an application programming interface (API) • PNAME = A program that was initated by support personnel

Viewing the maintenance log

About this task

The maintenance log contains descriptions of all reported maintenance events.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Logs** section, click **Maintenance**.
4. Enter appropriate information for the report.
5. Click **Display** to start the report.

Maintenance log field descriptions

Name	Description
Errors?	Select Yes if you want to display log entries with the event type ERR.
Resolutions?	Select Yes if you want to display log entries with the event type RES.
Events?	Select Yes if you want to display log entries with the event type EVN.
Start Date	Enter two numeric characters in the month, day, and year fields in the format mm/dd/yy. This displays the log for the specified date and beyond. You cannot specify dates before 1970 or after 2037. The year field requires 2 characters. The numbers 00 - 37 represents the years 2000 - 2037, and numbers 70 - 99 represents the years 1970 - 1999.

Table continues…

Name	Description
Time	This displays the logs for the specified time going forward. If no time is specified, the time starts from the beginning of the day, indicated as 00:00:00, for the specified date. This field takes 24–hour clock time in the format hh:mm:ss. If only the time is specified, the start date is the current day.
Application	The two-character code that identifies each module in the system: EL = Enhanced-List Application IM = Internet Messaging LD = LDAP MT = Maintenance SM = Station Manager VM = Messaging (voice mail, fax mail, and email messages) VP = Voice Platform You can also select ALL to display the appropriate entries for all applications.
Event ID	A code that identifies the condition reported. Only those log entries with the specified Event ID are displayed.
Problem Resource Type	The problem resource type. This identifies the logical resource type or system component reported. Only log entries with the specified problem resource type are displayed.
Reporting Resource Type	The reporting resource type. This identifies the logical resource type of the resource that discovers and detects the problem. Only log entries with the specified reporting resource type are displayed.
Reporting Resource Source	The reporting resource source. This is a unique value that is used to identify the specific line of code reporting the condition. Only log entries with the specified reporting resource source are displayed.
Search String	A text string used for searching for logs. Only log entries that contain the specified text entries are displayed.

Overview of traffic reports

Traffic reports serve several purposes. The reports help you to:

- Determine the grade of service (GOS) provided to subscribers during the busy hour at your site.
- Determine the port usage on the messaging system in daily or hourly periods. You must run these reports periodically to monitor performance and to anticipate your system's needs.
- Determine if your messaging system is performing at peak efficiency by providing actual usage information that you can compare with the type of usage that was initially forecast for your system.
- Troubleshoot administration problems that can occur with subscribers and equipment as system usage increases and requirements change.

Traffic reports also provide the following information about outcalling ports, subscriber traffic, and feature traffic that help you evaluate system efficiency.

Archiving traffic reports

If you print messaging traffic reports regularly and file them sequentially by date, they can provide an ongoing audit and historical reference of your messaging system. These reports can be useful for analyzing trends and tracking system performance over a period of time. Traffic records collected for a specific day, hour, or month are retained on the system only for a limited number of days, hours, or months. Therefore, you must run and print the reports regularly to ensure that you maintain a complete record from one reporting period to the next. See Data Retention Requirements on page 214 for more information about how long the system retains traffic records.

Printing traffic reports

To print the contents of any messaging administration screen, go to the **Reports** section and click **Measurements**. After you generate a report, click the Print button on the toolbar of your browser.

Listing of traffic reports

Each application on the messaging system provides its own set of reports for tracking data that is relevant and specific to the application itself. The following table lists each traffic report and its purpose. To see more information about a report, click the procedure link.

Report	Purpose	Procedure Link
Digital Networking		
Network Load Traffic (Hourly/Daily)	Displays the number of calls handled by each active messaging Digital Networking port within a reporting period.	Network Load Daily Traffic Report on page 227 or Network Load Hourly Traffic Report on page 228
Remote Messages Traffic (Monthly/Daily)	Displays up to 13 months' worth of information about the traffic load between a local messaging system and a specified remote messaging system.	Remote Messages Daily Traffic Report on page 229 or Remote Messages Monthly Traffic Report on page 232
Traffic-Snapshot	The total traffic for all the machines with the specified connection type. Also displays the total number of updates.	Traffic-Snapshot Daily Report or Traffic-Snapshot Monthly Report

Preparing the system for traffic reports

Before you can run a report, you must define the features and requirements for that report. The messaging system gathers data according to the requirements that you set.

Activating the collection of traffic data

About this task

The messaging system must start collecting traffic data before the system can format that data into a report. Reports can be produced for the current day or hour. Therefore, you can start running traffic reports almost as soon as traffic collection is activated. However, data for the full range of reporting periods (such as 192 hours, 8 days, or 13 months, depending on the report) is not available until that many hours', days', or months' worth of traffic data has been collected.

Procedure

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

   The system displays the Administer System Attributes and Feature page.
4. In the **Miscellaneous Parameters** section, enter values in the **System Prime Time, Start**, and **End** fields to indicate the window that will be used by the system to analyze and report prime-time traffic data.

   These values correspond to your company's business hours but can be set to any values you want. Traffic data is also collected at other times, but for reporting purposes, these values designate the prime-time hours.

   Note:

   The values you enter in these fields affect other system features, such as determining when out-of-hours personal greetings are played and routing out-of-hours calls to automated attendants. Be sure that any changes you make here do not adversely affect other feature functionality.
5. In the **Feature Activations** section, ensure that the **Traffic Collection?** field has **Yes**.
6. Click **Save**.

Data retention requirements

When traffic collection is activated, the messaging system stores the present collection record and records of previous consecutive collection periods. How long each record is retained depends on the type of report, as follows:

- Traffic records that contain daily information for the feature, load, community, net load, and special features reports are stored for 32 consecutive days.

  For example, if today is January 1, the present record contains the traffic data collected today, along with the previous 31 daily records, starting with December 31 (yesterday) and going back to December 1.
- Traffic records that contain daily information for the remote messages and subscriber reports are stored for 8 consecutive days.

  For example, if today is Monday, the present record contains the traffic collected today, along with the previous 7 daily records, starting with Sunday (yesterday) and going back to the previous Monday.
- Traffic records that contain hourly information for the community, feature, load, and special features reports are stored for 192 consecutive hours, which equals 8 days of hourly information.

For example, if the time is 8:15 a.m., the present record contains the traffic records collected since 8:00 a.m., along with the previous 191 hourly records, starting with 7:00 a.m. and going backwards.

- Traffic records that contain monthly information for the remote messages and subscriber reports are stored for 13 consecutive months.

  For example, if today is January 15, the present record contains the traffic collected so far this month, along with the previous 12 monthly records, starting with December (last month) and going back to the previous January.

As each new traffic record is collected, the oldest record is deleted. Therefore, you must produce traffic reports on a regular and timely basis, or you will lose the information that the reports make available to you. This is especially true if you retain the reports for historical purposes, such as for a performance audit or for comparative analysis.

Running traffic reports

To run the traffic reports, type the command for the report that you want on the command line. Include the start date or month, or the starting hour or traffic type, depending on the report. In a few seconds, the system formats the collected data into the specified report. The table for Traffic Reports on page 263 contains a list of available reports.

Note:

If you do not enter a specific start date or time, you receive a report for the current day, month, or hour.

Community Daily Traffic Report

The Community Daily Traffic report shows daily measurements of messages that were sent and received by each community.

Report Contents

The report shows the total number of messages that were sent and received by each community. It also shows the number of messages that were not sent or received by each community due to restrictions on sending during any day in the 32-day period, including the current date.

Viewing the Community Daily Traffic report

About this task

If you use the Sending Restrictions feature, the Community Daily Traffic report monitors the feature's effectiveness and provides data for you to check to ensure that the appropriate communities in your organization are restricted. For example, if a community has a large number of calls that are blocked due to restrictions on sending, you might want to investigate further to determine if there is:

- An administration problem. Are the correct communities being allowed or denied access?
- A subscriber problem. Do subscribers know that they are restricted, and is the restriction appropriate?

Also, depending on how you use the feature, this report can provide security information if you are monitoring call activity involving sensitive communities.

To run a Community Daily Traffic report:

You can view the traffic by community for a selected frequency; daily or hourly.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Community**.
5. In the **Cycle** field, click **Daily**.
6. In the **Start Date** field, enter a date.

   You can select a date in the mm/dd/yy format. The date can be up to 31 days prior to the current date that you want as a starting point for the report. If you enter a date, the report displays one screen of traffic information for each day from the start date to the current date. If you do not enter a date, today's traffic information is displayed.
7. Click **Get Report**.

   The system displays the Community Daily Traffic report.

   Note:

   To clear a generated report on the page, click **Clear**.

Community Daily Traffic field descriptions

Name	Description
Start Date	The starting date for which traffic data was collected for the report. It is the date you entered on the command line, or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Prev Day** and **Next Day** to scroll through each daily report record.
Ending Time	The time at which data collecting ended or the current time if the current hour is being reported.
Community ID	The communities that you administered for subscribers or for classes of service.
Sent by	The total number of messages that were sent by each community during the reporting period.
Received by	The total number of messages that were received by each community during the reporting period.
Not Sent by	The total number of messages that each community attempted to send during the reporting period but for which delivery failed due to sending restrictions.

Table continues…

Name	Description
Not Received by	The total number of messages that were addressed to members of the indicated community by members of another community during the reporting period but were not received due to sending restrictions.

Community Hourly Traffic report

The Community Hourly Traffic report shows an hourly measure of messages that were sent and received by each community.

Report contents

The report shows the total number of messages that were sent and received by each community. It also shows the number of messages that were not sent or received by each community due to restrictions on sending during any hour in the 192-hour (eight day) period, including the current hour.

Viewing the Community Hourly Traffic report

About this task

If you use the Sending Restrictions feature, the Community Hourly Traffic report monitors the feature's effectiveness and provides data to ensure that the appropriate communities in your organization are restricted. For example, if a community has a large number of calls that are blocked by sending restrictions, you might want to investigate further to determine if there is:

- An administration problem. Are the correct communities being allowed or denied access?
- A subscriber problem. Do subscribers know that they are restricted, and is the restriction appropriate?

Also, depending on how you use the feature, this report can provide security information if you are monitoring call activity involving sensitive communities.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Community**.
5. In the **Cycle** field, click **Hourly**.
6. In the **Start Date** field, enter a starting date up to 7 days prior to the current date in mm/dd/yy format.

   You must specify a date before you can specify an hour. The report displays one screen of traffic information for each hour. If you do not enter a date, the current date is used. If you do not enter an hour, the current hour of the current date is used.
7. In the **Hour** field, click the hour from which data for the report must begin.

   You can specify 24-hour time up to 191 hours prior to the current hour.

8. Click **Get Report**.

Community Hourly Traffic report field descriptions

Name	Description
Start Date	The starting date for which traffic data was collected for the report. It is the date you entered on the command line, or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Hour** and **Prev Hour** to scroll through each hourly report record.
Hour	The hour for which traffic data was collected for the report. You can specify 24-hour time up to 191 hours prior to the current hour.
Ending Time	The time at which data collecting ended or the current time if the current hour is being reported.
Community ID	The communities that you administered for subscribers or for classes of service.
Sent by	The total number of messages that were sent by each community during the reporting period.
Received by	The total number of messages that were received by each community during the reporting period.
Not Sent by	The total number of messages that each community attempted to send during the reporting period but for which delivery failed due to sending restrictions.
Not Received by	The total number of messages that were addressed to members of the indicated community by members of another community during the reporting period but were not received due to sending restrictions.

Viewing Feature Daily Traffic report

About this task

The Feature Daily Traffic report shows traffic information on a feature-by-feature basis. Features are divided into call answer features and messaging features.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Feature**.
5. In the **Cycle** field, click **Daily**.
6. In the **Start Date** field, enter a date up to 7 days prior to the current date.
7. Click **Get Report**.

   This report records two screens of traffic information for each day.

Feature Daily Traffic field descriptions

Name	Description
Start Date	The starting date for which traffic data was collected for the report. It is the date that you entered on the command line or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Day** and **Prev Day** to scroll through each daily report record.
Ending Time	The time at which data collecting ended.
VOICE MAIL	
Total Messages, Sent	The total number of messages that were sent on the local messaging system during the reporting period. **Note:** The Message Sent count includes all messages that were created on the local machine, including header-only messages, messages to remote subscribers, unaddressed messages, undeliverable messages, and remote incoming messages. A message sent to a mailing list counts as one message created for each recipient.
Total Messages, Current	The total number of messages that are presently residing on the local messaging system. **Note:** The traffic unavailable display is normal.
Voice Components, Sent **Voice Components, Current**	The total number of voice components that were sent on the local messaging system during the reporting period. The Voice Components Sent count is the total number of voice components included in all messages that were created on the local machine, including messages to remote subscribers, unaddressed messages, undeliverable messages, and remote incoming messages. The total number of voice components that are presently residing on the local messaging system.
FAX Components, Sent **FAX Components, Current**	The total number of faxes that were sent on the local messaging system during the reporting period. The total number of faxes that are presently residing on the local messaging system.
Binary Attachments, Sent **Binary Attachments, Current**	The total number of binary attachments that were sent on the local messaging system during the reporting period. The Binary Attachments Sent count is the total number of binary attachments included in all messages that were created on the local machine, including messages to remote subscribers, unaddressed messages, undeliverable messages, and remote incoming messages.

Table continues…

Name	Description
	The total number of binary attachments that are presently residing on the local messaging system.
Text Components, Sent **Text Components, Current**	The total number of text components that were sent on the local messaging system during the reporting period. The Text Components Sent count is the total number of text components included in all messages that were created on the local machine, including messages to remote subscribers, unaddressed messages, undeliverable messages, and remote incoming messages. The total number of text components that are presently residing on the local messaging system.
Broadcast Messages, Sent	The number of broadcast messages (as defined by the broadcast messages feature) that were sent on the local messaging system during the reporting period.
Broadcast Messages, Current	The number of messages that are presently residing in the broadcast mailbox on the local messaging system that are marked as broadcast messages.
Log-in Announcement, Sent	The number of messages sent on the local messaging system during the reporting period that were login announcements (as defined by the login announcement feature).
Log-in Announcements, Current	The number of messages that are presently residing in the broadcast mailbox on the local messaging system that are marked as login announcements. Since only one login announcement can exist at any one time in the broadcast mailbox, this number is always 0 or 1.
Priority Messages, Sent	The number of messages sent on the local messaging system during the reporting period that were marked for priority delivery. The Priority Messages Sent count includes all priority messages that were created on the local machine, including header-only messages, messages to remote subscribers, unaddressed messages, undeliverable messages, and remote incoming messages. A message sent to a mailing list counts as one message created for each recipient.
Priority Messages, Current	The number of messages that are presently residing on the local messaging system that are marked as priority messages.
Private Messages, Sent	The number of messages sent on the local messaging system during the reporting period that were marked for private delivery. The Private Message Sent count includes all private messages that were created on the local machine, including header-only messages, messages to remote subscribers, unaddressed messages, undeliverable messages, and remote incoming messages. A message sent to a mailing list counts as one message created for each recipient.
Private Messages, Current	The number of messages that are presently residing on the local messaging system that are marked for private delivery.

Table continues…

Name	Description
Avg. Storage Time	The average duration (in minutes) for the hour being reported that messages remained in mailboxes before they were deleted.
Avg. Connect Time	The average duration (in seconds) of calls made directly to a mailbox that occurred during the reporting period.
CALL ANSWER	
Total Messages, Received	The number of call answer messages that were recorded or received by the local machine during the reporting period.
Total Messages, Current	The number of call answer messages that are presently stored in the local messaging system.
Voice Components, Received **Voice Components, Current**	The number of call answer voice components that were recorded on the local machine during the reporting period. The number of call answer voice components that are presently stored in the local messaging system.
FAX Components, Received **FAX Components, Current**	The number of fax messages that were recorded or received by the local machine during the reporting period. The number of faxes that are presently stored in the local messaging system.
Avg. Storage Time	The average duration (in minutes) during the day being reported that call answer messages were stored in mailboxes before they were deleted.
Avg. Connect Time	The average duration (in seconds) of call answer calls that were made during the reporting period.
Maximum Average Voice Ports in Use	
Maximum Average IMAPI Sessions in Use	
SUBSCRIBERS	Local, Remote, Non Administered Remote
VOICE MAIL	Successful Logins External, Successful Logins Internal, Successful Logins Client Logins, Failed Logins External, Failed Logins Internal, Failed Logins Client Logins, Session Usage (Seconds), Session Usage.
CALL ANSWER	Completed Calls External, Completed Calls Internal, Completed Calls Network, Voice Components External, Voice Components Internal, Voice Components Network, FAX Components External, FAX Components Internal, FAX Components Network, Abandoned Calls External, Abandoned Calls Internal, Abandoned Calls Network, Session Usage (Seconds), Session Usage.

Viewing Feature Hourly Traffic report

About this task

The Feature Hourly Traffic report shows traffic information on a feature-by-feature basis. Features are divided into call answer features and messaging features.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Feature**.
5. In the **Cycle** field, click **Hourly**.

   The date specification precedes an hour specification. If you do not enter a date, the current date is used. If you do not enter an hour, the current hour of the current date is used. The report displays one screen of traffic information for each hour.
6. In the **Start Date** field, enter a date in mm/dd/yy format.

   The starting date can be up to seven days before the current date.
7. In the **Hour** field, select a time from which the report must begin.
8. Click **Get Report**.

   The system displays the Feature Hourly Traffic page. The fields on the page are identical to those on the Feature Daily Traffic page.

   This report records two screens of traffic information for each hour.

Feature Hourly Traffic field descriptions

Name	Description
Start Date	The starting date for which traffic data was collected for the report. It is the date that you entered on the command line or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Hour** and **Prev Hour** to scroll through each hourly report record.
Hour	The starting hour for which traffic data was collected for the report. It is the hour you entered on the command line or the current hour if you did not specify an hour.
Ending Time	The time at which data collecting ended.
Average Voice Ports in Use	The average number of voice ports that were in use simultaneously during the hour of the day you selected. On small systems, if this number is greater than half the total number of ports configured, the messaging system is probably experiencing call blocking.
Average IMAPI Sessions in Use	The average number of IMAPI sessions that were in use simultaneously during the hour of the day you selected. On small systems, if this number is greater than half the total number of ports configured, the messaging system is probably experiencing call blocking.
SUBSCRIBERS	

Table continues…

Name	Description
Local	The total number of local subscribers who were administered on the messaging system at the end of the hour being reported.
Remote	The total number of remote subscribers who were administered on the messaging system at the end of the hour being reported.
Non Administered Remote	The total number of subscribers external to the messaging system (not administered) who sent mail to an administered messaging subscriber or to whom mail was sent by an administered messaging subscriber the end of the hour being reported.
VOICE MAIL	
Successful Logins, External **Successful Logins, Internal** **Successful Logins, Client Logins**	The number of successful login attempts that were made during the hour reported. Login attempts were made by subscribers calling from: • Telephones not administered (external) on the host switch • Telephones administered (internal) on the host switch • IMAPI interface (client logins)
Failed Logins, External **Failed Logins, Internal** **Failed Logins, Client Logins**	The number of unsuccessful login attempts made during the hour reported. Login attempts were made by subscribers calling from: • Telephones not administered (external) on the host switch • Telephones administered (internal) on the host switch • MCAPI interface (client logins) Unsuccessful means that the messaging system did not allow the caller access to messaging operations. Denial to access could be due to an unrecognizable password, login ID, or both, or because the caller hung up before completing the call.
Session Usage (seconds)	The total number of seconds (across all ports) that the system was used for messaging sessions (including voice messages, call message retrieval, change of passwords, and changes of personal greetings) during the hour being reported.
Session Usage	The total number of seconds that IMAPI sessions were in use for voice mail sessions during the hour reported.
CALL ANSWER	
Completed Calls, External **Completed Calls, Internal** **Completed Calls, Network**	The number of completed call answer telephone calls that were made to the messaging system during the hour reported. Calls came from: • Telephones not administered (external) on the host switch • Telephones administered (internal) on the host switch • Telephones networked with IMAPI sessions to the host switch These numbers include the times that the messaging system answered calls for subscribers, attendants, and bulletin boards.

Table continues…

Name	Description
Voice Components, External **Voice Components, Internal** **Voice Components, Network**	The number of voice components that were included in call answer telephone calls made to the messaging system during the hour reported. Calls came from: • Telephones not administered (external) on the host switch • Telephones administered (internal) on the host switch • Telephones networked with IMAPI sessions to the host switch These numbers include the times that the messaging system answered calls for subscribers, attendants, and bulletin boards.
FAX Components, External **FAX Components, Internal** **FAX Components, Network**	The number of faxes that were included in call answer telephone calls made to the messaging system during the hour reported. Calls came from: • Telephones not administered (external) on the host switch • Telephones administered (internal) on the host switch • Telephones networked with IMAPI sessions to the host switch These numbers include the times that the messaging system answered calls for subscribers, attendants, and bulletin boards.
Abandoned Calls, External **Abandoned Calls, Internal** **Abandoned Calls, Network**	The number of times that a caller hung up after the mailbox greeting started to play, but before the beep, to leave a message. Calls came from: • Telephones not administered (external) on the host switch • Telephones administered (internal) on the host switch • Telephones networked with IMAPI sessions to the host switch These numbers include the times that the messaging system answered calls for subscribers, attendants, and bulletin boards.
Session Usage (seconds)	The total number of seconds (across all ports) that the system was used for call answer sessions during the hour being reported.
Session Usage	The total number of seconds that IMAPI sessions were used for call answer sessions during the hour being reported.

Viewing Load Daily Traffic report

About this task

The Load Daily Traffic report shows daily load traffic information for 1 to 32 days. Traffic load refers to the number of calls handled by each active port during the reporting period. Port usage measurements indicate how the ports are actually being used.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports**, click **Measurements**.
4. In the **Type** field, click **Load**.

5. In the **Cycle** field, click **Daily**.
6. In the **Start Date** field, enter a date in the mm/dd/yy field.
7. Click **Get Report**.

Load Daily Traffic field descriptions

Name	Description
Port Usage Data (Seconds)	The number of seconds that each port was in use during the reporting period. This report displays 64 peg count values, corresponding to ports 1 to 64.
Port Peg Count Data (Number of Calls)	The number of calls that each port handled during the reporting period. This report displays 64 peg count values, corresponding to ports 1 to 64.

Viewing Load Hourly Traffic report

About this task

The Load Hourly Traffic report shows hourly load traffic information for up to 192 hours (8 days). Traffic loadis the number of calls handled by each active port during the reporting period. Port usage measurements indicate how the ports are being used.

To run a Load Hourly Traffic report:

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Load**.
5. In the **Cycle** field, type **Hour**.
6. In the **Date** field, enter a date.

   The date in this field can be up to 7 days prior to the current date. To enter an hour, you must first enter a date. If you do not enter a date, the current hour of the current date is used. If you do not enter an hour, the report starts with the first hour of the date specified.
7. In the **Hour** field, enter the time.

   The time in this field can be up to 191 hours prior to the current hour.
8. Click **Get Report**.

Load Hourly Traffic report field descriptions

Field Name	Description
Start Date	The starting date for which traffic data was collected for the report. It is the date that you entered on the command line or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Hour** and **Prev Hour** to scroll through each hourly report record.
Hour	The starting hour for which traffic data was collected for the report. It is the hour that you entered on the command line or the current hour if you did not specify an hour.
Ending Time	The time at which data collecting ended.
TOTAL SUBSCRIBER THRESHOLD EXCEPTIONS	
Lists	The number of warnings that were issued to subscribers who exceeded the maximum allowable number of mailing lists during the period being reported.
List Space	The number of warnings that were issued to subscribers who exceeded the maximum allowable number of list entries during the period being reported.
Message Space, Lower	The number of warnings that were issued to subscribers to indicate that they had reached the lower space threshold during the period being reported. This lower threshold is set in the Thresholds screen.
Message Space, Upper	The number of warnings that were issued to subscribers to indicate that they had reached the upper space threshold during the period being reported. This upper threshold is set in the Thresholds screen.
Subscribers Over Threshold	The number of subscribers that exceeded one or more of the message space thresholds during the period being reported.
Deliveries Rescheduled	The number of message deliveries that could not be completed and were subsequently rescheduled or canceled.
Maximum Simultaneous Voice Ports	The greatest number of ports that were in use at any one time during the period being reported.
Maximum Simultaneous IMAPI Sessions	The greatest number of IMAPI sessions that were in use at any one time during the period being reported.
SYSTEM STORAGE	
Total Storage, Used (hours) **Total Storage, Free (hours)**	The maximum number of hours that was in use in all the voice text file systems during the period being reported (or the current number of hours in use if the current hour is being reported).
Message Storage	The maximum number of hours that was in use for all the messages during the time period being reported (or the current amount of free space available if the current hour is being reported).
Voiced Name Storage	The maximum number of hours that was in use for all the names during the time period being reported (or the current amount of free space available if the current hour is being reported)

Table continues…

Field Name	Description
% Remote	The percentage of the name storage that was used to store remote names.
Announcement Storage	The maximum number of hours in use for the announcement during the time period being reported.
SYSTEM STORAGE	Translation Storage, Miscellaneous Storage.
Port Usage Data (Seconds)	The port usage data in terms of number of seconds.
Port Peg Count Data (Number of Calls)	The port peg count data in terms of number of calls.

Viewing the Network Load Daily Traffic report

About this task

The Network Load Daily Traffic report shows network channel traffic one day at a time for up to 32 days. This report can show any nodes that are exceeding specified threshold limits, the number of calls that went unanswered, the number of calls on each channel, and other channel traffic information.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Network-Load**.
5. In the **Cycle** field, click **Daily**.
6. In the **Start Date** field, enter a date in mm/dd/yy format.

   The starting date can be up to 31 days prior to the current date.
7. Click **Get Report**.

   The system displays the Network Load Daily Traffic screen.

Network Load Daily Traffic report field descriptions

Name	Description
Start Date	The starting date for which traffic data was collected for the report. It is the date that you entered on the command line or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Day** and **Prev Day** to scroll through each daily report record.
Ending Time	The time at which data collecting ended.

Table continues…

Name	Description
Total Message Transmission Threshold Exceptions	The number of times that any node exceeded the specified message transmission threshold during the recording period.
Total Message Transmission Limit Exceptions	The number of times that any node exceeded the message transmission limit specified for that node during the recording period.
Remote Deliveries Rescheduled	The number of messages that were rescheduled because of transmission difficulties or space limitations on the remote node during the recording period.
Total Remote Undeliverable Messages	The total number of messages that were rejected for delivery to a remote machine because, for example, the remote subscriber was not defined to the local machine.
USAGE (SECONDS)	
Incoming **Outgoing** **Total**	The number of seconds that each network channel was active with incoming and outgoing calls during the recording period. The total seconds of activity are also provided.
PEG COUNT (NUMBER OF SESSIONS)	
Incoming **Outgoing** **Total**	The number of incoming and outgoing calls on each network channel during the recording period. The total number of calls is also provided.

Viewing the Network Load Hourly Traffic report

About this task

The Network Load Hourly Traffic report shows network channel traffic 1 hour at a time for up to 192 hours (8 days). This report can show any nodes that are exceeding specified threshold limits, the number of calls that went unanswered, the number of calls on each channel, and other channel traffic information.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Network-Load**.
5. In the **Cycle** field, click **Hourly**.
6. In the **Start Date** field, enter a date.

   The date can be up to 7 days prior to the current date.
7. In the **Hour** field, enter the time.

   The time can be 24-hour time up to 191 hours prior to the current hour, from which the data for the report must begin.

You must specify a date before specifying the hour. If you do not enter a date, the current date is used. If you do not enter an hour, the current hour of the current date is used.

8. Click **Get Report**.

Network Load Hourly Traffic report field descriptions

Name	Description
Start Date	The starting date for which traffic data was collected for the report. It is the date that you entered on the command line or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Hour** and **Prev Hour** to scroll through each hourly report record.
Hour	The starting hour for which traffic data was collected for the report. It is the hour that you entered on the command line or the current hour if you did not specify an hour.
Ending Time	The time at which data collecting ended.
Total Message Transmission Threshold Exceptions	The number of times that any node exceeded the specified message transmission threshold during the recording period.
Total Message Transmission Limit Exceptions	The number of times that any node exceeded the message transmission limit specified for that node during the recording period.
Remote Deliveries Rescheduled	The number of messages that were rescheduled because of transmission difficulties or space limitations on the remote node during the recording period.
Total Remote Undeliverable Messages	The total number of messages that were rejected for delivery to a remote machine because, for example, the remote subscriber was not defined to the local machine.
USAGE (SECONDS)	
Incoming **Outgoing** **Total**	The number of seconds that each network channel was active with incoming and outgoing calls during the recording period. The total seconds of activity are also provided.
PEG COUNT (NUMBER OF SESSIONS)	
Incoming **Outgoing** **Total**	The number of incoming and outgoing calls on each network channel during the recording period. The total number of calls is also provided.

Viewing the Remote Messages Daily Traffic report

About this task

The Remote Messages Daily Traffic report gathers up to 8 days of information about traffic load between a local messaging system and a specified remote messaging system .

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Remote-Messages**.
5. In the **Cycle** field, click **Daily**.
6. In the **Start Date** field, enter a date up to 7 days before the current date.

   If you do not enter a date, the system uses the current date.
7. Click **Get Report**.

   The system displays the remote machine.
8. Select the Remote Machine.
9. Click **Get Report**.

Remote Messages Daily Traffic field descriptions

Name	Description
Machine Name	The name of the remote machine that you entered on the command line.
Machine Type	The type of remote machine, for example, calld, messaging, and so on.
Start Date	The starting date for which traffic data was collected for the report. It is the date that you entered on the command line or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Day** and **Prev Day** to scroll through each daily report record.
Ending Time	The time at which data collecting ended.
LOCAL ORIGINATION	
Prime/Non-Prime	Whether message transmission came from the local messaging system during a period specified as prime or nonprime time.
Transfer Sessions	The number of message transfer sessions that occurred during the reporting period.
Usage (seconds)	The total number of seconds for all message transfer sessions that occurred during the reporting period.
Average Usage	The average length, in seconds, of a message transfer session.
Messages Sent	The total number of messages that were sent from the local messaging system to the remote messaging system.
Voice Components	The total number of voice components that were sent from the local messaging system to the remote messaging system.

Table continues…

Name	Description
FAX Components	The total number of faxes that were sent from the local messaging system to the remote messaging system.
Binary Attachments	The total number of binary attachments that were sent from the local messaging system to the remote messaging system.
Text Components	The total number of text components that were sent from the local messaging system to the remote messaging system.
Messages Rejected	The total number of messages that were rejected by the local messaging system during the reporting period. For call delivery machines, if there is no positive confirmation, the message is recorded as rejected.
Status Sent	The total number of status reports that were sent by the local messaging system to the remote messaging system for messages originated by the remote messaging system. This number equals 0 for call delivery machines.
Status Received	Not applicable.
Admin Updates	The total number of administration updates (name, voice name, extension, community changes, add and delete local subscribers) that were sent from the local messaging system to the remote messaging system. This field applies to digital network machines only.
REMOTE ORIGINATION	
Prime/Non-Prime	Whether message transmission came from the remote messaging system during a period specified as prime or nonprime time.
Transfer Sessions	The number of message transfer sessions that occurred during the reporting period.
Usage (seconds)	The total number of seconds for all message transfer sessions that occurred during the reporting period.
Average Usage	The average length, in seconds, of a message transfer session.
Messages Sent	The total number of messages that were sent from the remote messaging system and received by the local messaging system during the reporting period.
Voice Components	The total number of voice components that were sent from the remote messaging system and received by the local messaging system during the reporting period.
FAX Components	The total number of faxes that were sent from the remote messaging system and received by the local messaging system during the reporting period.
Binary Attachments	The total number of binary attachments that were sent from the remote messaging system and received by the local messaging system during the reporting period.
Text Components	The total number of text components that were sent from the remote messaging system and received by the local messaging system during the reporting period.
Messages Rejected	The total number of messages that were rejected by the local and remote messaging systems during the reporting period. For call delivery machines, if there is no positive confirmation, the message is recorded as rejected.

Table continues…

Name	Description
Status Sent	Not applicable.
Status Received	The total number of status reports that were received by the local messaging system for messages that the local machine sent to the remote messaging system.
Admin Updates	The total number of administration updates (name, voice name, extension, community changes, add and delete local subscribers) that were sent from the remote messaging system to the local messaging system. This field applies to digital network machines only.
Message Transmission Threshold Exceptions	The number of times that the local node exceeded its message transmission threshold.
Session Failures Far End "No Answer"	The number of unsuccessful call attempts from the local messaging system to the remote messaging system.

Viewing the Remote Messages Monthly Traffic report

About this task

The Remote Messages Monthly Traffic report gathers up to 13 months of information about traffic load between a local messaging system and a specified remote messaging system.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Remote-Messages**.
5. In the **Cycle** field, click **Monthly**.

   The month can be up to 13 months before the current month.

   If no month is specified, the current month is used.
6. Click **Get Report**.

   The system displays the available remote machines.
7. Select the Remote Machine.
8. Click **Get Report**.

Remote Messages Monthly Traffic report field descriptions

Name	Description
Machine Name	The name of the remote machine that you entered on the command line.
Machine Type	The type of remote machine, for example, calld or messaging.

Table continues…

Name	Description
Start Date	The starting month for which traffic data was collected for the report. It is the month that you entered on the command line or the current date if you did not specify a month. If you enter a month prior to the current month, each month's record is presented as an additional page (screen). Click **Next Month** and **Prev Month** to scroll through each monthly report record.
Ending Time	The day on which data collection ended.
LOCAL ORIGINATION	
Prime/Non-Prime	Whether message transmission came from the local messaging system during a period specified as prime or nonprime time.
Transfer Sessions	The number of message transfer sessions that occurred during the reporting period.
Usage (seconds)	The total number of seconds for all message transfer sessions that occurred during the reporting period.
Average Usage	The average length, in seconds, of a message transfer session.
Messages Sent	The total number of messages that were sent from the local messaging system to the remote messaging system.
Voice Components	The total number of voice components that were sent from the local messaging system to the remote messaging system.
FAX Components	The total number of faxes that were sent from the local messaging system to the remote messaging system.
Binary Attachments	The total number of binary attachments that were sent from the local messaging system to the remote messaging system.
Text Components	The total number of text components that were sent from the local messaging system to the remote messaging system.
Messages Rejected	The total number of messages that were rejected by the local messaging systems during the reporting period. For call delivery machines, if there is no positive confirmation, the message is recorded as rejected.
Status Sent	The total number of status reports that were sent by the local messaging system to the remote messaging system for messages originated by the remote messaging system. This number is 0 for call delivery systems.
Status Received	Not applicable.
Admin Updates	The total number of administration updates (name, voice name, extension, community changes, add and delete local subscribers) that were sent from the local messaging system to the remote messaging system. This field applies to digital network systems only.
REMOTE ORIGINATION	
Prime/Non-Prime	Whether message transmission came from the remote messaging system during a period specified as prime or nonprime time.
Transfer Sessions	The number of message transfer sessions that occurred during the reporting period.

Table continues…

Name	Description
Usage (seconds)	The total number of seconds for all message transfer sessions that occurred during the reporting period.
Average Usage	The average length, in seconds, of a message transfer session.
Messages Sent	The total number of messages that were sent from the remote messaging system and received by the local messaging system during the reporting period.
Voice Components	The total number of voice components that were sent from the remote messaging system and received by the local messaging system during the reporting period.
FAX Components	The total number of Fax components that were sent from the remote messaging system and received by the local messaging system during the reporting period.
Binary Attachments	The total number of binary attachments that were sent from the remote messaging system and received by the local messaging system during the reporting period.
Text Components	The total number of text components that were sent from the remote messaging system and received by the local messaging system during the reporting period.
Messages Rejected	The total number of messages that were rejected by the local and remote messaging systems during the reporting period. For call delivery machines, if there is no positive confirmation, the message is recorded as rejected.
Status Sent	Not applicable.
Status Received	The total number of status reports that were received by the local messaging system for messages that the local machine sent to the remote messaging system.
Admin Updates	The total number of administration updates (name, voice name, extension, community changes, add and delete local subscribers) that were sent from the remote messaging system to the local messaging system. This field applies to digital network systems only.
Message Transmission Threshold Exceptions	The number of times that the local node exceeded its message transmission threshold.
Session Failures Far End "No Answer"	The number of unsuccessful call attempts from the local messaging system to the remote messaging system.

Viewing Special Features Daily Traffic report

About this task

The Special Features Daily Traffic report shows the outcalling traffic information (which includes outcalling, and message delivery) for any day during the most recent 32-day collection period.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.

4. In the **Type** field, click **Special Features**.
5. In the **Cycle** field, click **Daily**.
6. In the **Start Date** field, enter a date up to 31 days before the current date.
7. Click **Get Report**.

Special Features Daily Traffic field descriptions

Name	Description
Start Date	The starting date for which traffic data was collected for the report. It is the date that you entered on the command line or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Day** and **Prev Day** to scroll through each daily report record.
Ending Time	The time at which data collecting ended.
Maximum Simultaneous Outcalls	The largest number of ports that were simultaneously used for outcalling during the reporting period.
Outcalls Attempted	The number of outcalls that were tried during the reporting period.
Outcalls Completed	The number of successful outcalls during the reporting period.
Outcalls Rescheduled	The number of outcalls that were rescheduled when an outcall attempt failed due to all ports being busy.
Calls Answered Without Connect	The number of calls that were answered without a switchlink connectmessage.

Viewing the Special Features Hourly Traffic report

About this task

The Special Features Hourly Traffic shows the outcalling traffic information, which includes outcalling, and message delivery for any hour during the most recent 192-hour (8-day) period.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Special-Features**.
5. In the **Cycle** field, click **Hourly**.
6. In the **Start Date** field, enter a date up to 7 days before the current date.
7. In the **Hour** field, enter a time up to 191 hours prior to the current hour.
8. Click **Get Report**.

Special Features Hourly Traffic field descriptions

Name	Description
Start Date	The starting date for which traffic data was collected for the report. It is the date that you entered on the command line or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Hour** and **Prev Hour** to scroll through each hourly report record.
Hour	The starting hour for which traffic data was collected for the report. It is the hour that you entered on the command line or the current hour if you did not specify an hour.
Ending Time	The time at which data collecting ended.
Maximum Simultaneous Outcalls	The largest number of ports that were simultaneously used for outcalling during the reporting period.
Outcalls Attempted	The number of outcalls that were tried during the reporting period.
Outcalls Completed	The number of successful outcalls during the reporting period.
Outcalls Rescheduled	The number of outcalls that were rescheduled when an outcall attempt failed due to all ports being busy.
Calls Answered Without Connect	The number of calls that were answered without a switchlink connect message.

Viewing the Subscriber Daily Traffic report

About this task

The Subscriber Daily Traffic report shows traffic information about a specific subscriber for any day within the most recent 8-day period. This report can help you track a particular subscriber's mail-usage patterns.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Subscriber**.
5. In the **Cycle** field, click **Daily**.
6. In the **Start Date** field, enter a date in the mm/dd/yy format.

   The starting date can be up to 7 days before the current date.

   If you do not enter a date, the system uses the current date.
7. Click **Get Report**.

8. In the **Enter Subscriber Extension** field, do one of the following:
   - Type the extension of the subscriber.
   - Type the name of the subscriber.

   Note:

   If the subscriber's name is administered in your system with an embedded space, such as Jane Doe, you must type the name enclosed in quotation marks, for example, “Jane Doe”.

9. Click **Get Report**.

   The system displays the Subscriber Daily Traffic report with four screens of traffic information for each day.

Subscriber Daily Traffic report field descriptions

Name	Description
Name	The name of the subscriber whose traffic information is being reported. It is the name that you entered on the command line or the name that corresponds to the subscriber's extension, if you entered the extension.
Extension	The extension of the subscriber whose traffic information is being reported. This is the extension you entered on the command line, or the extension that corresponds to the subscriber's name, if you entered the name.
Start Date	The starting date for which traffic data was collected for the report. It is the date that you entered on the command line or the current date if you did not specify a date. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Day** and **Prev Day** to scroll through each daily report record.
Ending Time	The time at which data collecting ended.
Community ID	The number of the community to which the subscriber belongs.
Mailbox Space Used	The amount of message space (in seconds) that was in use by the subscriber at the end of the period being reported.
Space Allowed	The maximum mailbox size (in seconds) that was administered for this subscriber during the reporting period.
Maximum Space Used	The maximum amount of message space (in seconds) that was in use at any given time during the reporting period.
Space Guaranteed	The minimum message space (in seconds), if any, guaranteed for the subscriber's mailbox during the reporting period.
CALL ANSWER **Sessions, Prime** **Sessions, Non-Prime**	The number of times that callers were redirected to the messaging system to leave a call answer message during prime and nonprime hours during the reporting period.

Table continues…

Name	Description
VOICE MAIL **Sessions, Prime** **Sessions, Non-Prime**	The number of times that the subscriber successfully logged in to the messaging system during prime and nonprime hours during the reporting period.
CALL ANSWER **Session Usage, Prime** **Session Usage, Non-Prime**	The total duration (in seconds) of calls to the subscriber during prime and nonprime hours during the reporting period.
VOICE MAIL **Session Usage, Prime** **Session Usage, Non-Prime**	The total duration (in seconds) of time that the subscriber was logged in to the messaging system during prime and nonprime hours during the reporting period.
VOICE MAIL MESSAGES RECEIVED	
Local Mail Messages, Prime **Local Mail Messages, Non-Prime**	The number of messages that were received by the subscriber during prime and nonprime hours during the reporting period.
Voice Components	The number of voice components that were received by the subscriber during prime and nonprime hours during the reporting period.
FAX Components	The number of Fax components that were received by the subscriber during prime and nonprime hours during the reporting period. .
Binary Attachments	The number of binary attachments that were received by the subscriber during prime and nonprime hours during the reporting period.
Text Components	The number of text components that were received by the subscriber during prime and nonprime hours during the reporting period.
Remote Mail Messages, Prime **Remote Mail Messages, Non-Prime**	The number of messages that were received by the subscriber from remote machines during prime and nonprime hours during the reporting period.
Voice Components	The number of voice components that were received by the subscriber from remote machines during prime and nonprime hours during the reporting period.
FAX Components	The number of Fax components that were received by the subscriber from remote machines during prime and nonprime hours during the reporting period.

Table continues…

Name	Description
Binary Attachments	The number of binary attachments that were received by the subscriber from remote machines during prime and nonprime hours during the reporting period.
Text Components	The number of text components that were received by the subscriber from remote machines during prime and nonprime hours during the reporting period.
Undeliverable Notifications, Prime **Undeliverable Notifications, NonPrime**	The number of times that a subscriber was alerted that a message was undeliverable during prime and nonprime hours during the reporting period.
CALL ANSWER MESSAGES RECEIVED	
Prime **Non-Prime**	The number of new call answer messages that accumulated in the subscriber's mailbox during prime and nonprime hours during the reporting period.
Voice Components	The number of new voice components that accumulated in the subscriber's mailbox during prime and nonprime hours during the reporting period.
FAX Components	The number of new Fax components that accumulated in the subscriber's mailbox during prime and nonprime hours during the reporting period.
MESSAGES CREATED	
Total Voice-Mail Messages, Prime **Total Voice-Mail Messages, NonPrime**	The total number of messages that were created by the subscriber during prime and nonprime hours during the reporting period.
Broadcast Messages, Prime **Broadcast Messages, Non-Prime**	The number of broadcast messages that were created by the subscriber during prime and nonprime hours during the reporting period.
Login Announcements, Prime **Login Announcements, Non-Prime**	The number of login announcements that were created by the subscriber during prime and nonprime hours during the reporting period.
Priority Messages, Prime **Priority Messages, Non-Prime**	The number of priority messages that were created by the subscriber during prime and nonprime hours during the reporting period.
Private Messages, Prime	The number of private messages that were created by the subscriber during prime and nonprime hours during the reporting period.

Table continues…

Name	Description
Private Messages,Non-Prime	
Voice Components	The number of voice components that were created by the subscriber during prime and nonprime hours during the reporting period.
FAX Components	The number of Fax components that were created by the subscriber during prime and nonprime hours during the reporting period.
Binary Attachments	The number of binary attachments that were created by the subscriber during prime and nonprime hours during the reporting period.
Text Components	The number of text components that were created by the subscriber during prime and nonprime hours during the reporting period.
MESSAGES SENT	
Local Messages, Prime **Local Messages, NonPrime**	The number of messages that were sent to local subscribers by the subscriber during prime and nonprime hours during the reporting period.
Voice Components	The number of voice components that were sent to local subscribers by the subscriber during prime and nonprime hours during the reporting period.
FAX Components	The number of Fax components that were sent to local subscribers by the subscriber during prime and nonprime hours during the reporting period.
Binary Attachments	The number of binary attachments that were sent to local subscribers by the subscriber during prime and nonprime hours during the reporting period.
Text Components	The number of text components that were sent to local subscribers by the subscriber during prime and nonprime hours during the reporting period.
Remote Messages, Prime **Remote Messages, Non-Prime**	The number of messages that were sent to remote subscribers by the subscriber during prime and nonprime hours during the reporting period.
Voice Components	The number of voice components that were sent to remote subscribers by the subscriber during prime and nonprime hours during the reporting period.
FAX Components	The number of fax components that were sent to remote subscribers by the subscriber during prime and nonprime hours during the reporting period.
Binary Attachments	The number of binary attachments that were sent to remote subscribers by the subscriber during prime and nonprime hours during the reporting period.
Text Components	The number of text components that were sent to remote subscribers by the subscriber during prime and nonprime hours during the reporting period.

Viewing the Subscriber Monthly Traffic report

About this task

The Subscriber Daily Traffic report shows traffic information about a specific subscriber for any month within the most recent 12-month period. This report can help you track a particular subscriber's mail-usage patterns.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Subscriber**.
5. In the **Cycle** field, click **Monthly**.
6. In the **Start Date** field, enter a month in the mm/yyyy format.

   The starting month can be up to 12 months before the current month.

   If you do not specify a month, the current month is used
7. Click **Get Report**.
8. In the **Enter Subscriber Extension** field, do one of the following:
   - Type the extension of the subscriber.
   - Type the name of the subscriber.

     Note:

     If the subscriber's name is administered in your system with an embedded space, such as Jane Doe, you must type the name enclosed in quotation marks, for example, “Jane Doe”.
9. Click **Get Report**.

Result

The system displays the Subscriber Monthly Traffic report with four screens of traffic information for every month. The fields for this report are identical to the fields for the Subscriber Daily Traffic report.

Viewing the Traffic Snapshot Daily report

About this task

The Traffic Snapshot Daily report shows all of the traffic data that occurred on your messaging system during a specific day. This report shows all incoming and outgoing traffic for local machines and remote machines.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Traffic-Snapshot**.
5. In the **Cycle** field, click **Daily**.
6. In the **Start Date** field, enter a date in the mm/dd/yyyy format.

   If you do not enter a date, the system uses the current date.
7. Click **Get Report**.
8. In the **Select connection type** field, click a network connection type.
9. Click **Get Report**.

Result

The system displays the Traffic Snapshot Daily report with the traffic for each remote machine of the connection type you selected.

Traffic Snapshot Daily report field descriptions

Name	Description
Connection Type	The type of network connection: • Digital = rs232, dcp, or tcp/ip
Start Date	The day of the traffic data; either the date you entered on the command line or the current date.
Ending Time	The hour and minute that the system stopped collecting data.
TRAFFIC TOTAL	
MESSAGES, Sent	The total number of messages that the local machine sent to all remote machines with this connection type.
MESSAGES, Received	The total number of messages that the local machine received from all remote machines with this connection type.
UPDATES, Out	The total number of updates that the local machine sent to all remote machines (for digital connection types only). Examples of updates are: name, extension, community ID.
UPDATES, In	The total number of updates that the local machine received from all remote machines (for digital connection types only). Examples of updates are: name, extension, community ID.
TRNSFR SESS, Prime	The total number of transfer sessions with this connection type that occurred during prime time.

Table continues…

Name	Description
TRNSFR SESS, Non-P	The total number of transfer sessions with this connection type that occurred before or after prime time.
% USAGE, Prime	The total percentage of usage for this connection type that occurred during prime time. This percentage is the sum of all machine usage. (See the % USAGE, Prime field below.)
% USAGE, Non-P	The total percentage of usage for this connection type that occurred before or after prime time. This percentage is the sum of all machine usage. (See the % USAGE, Non-P field below.)
MESSAGES, Queued	The total number of messages that are currently in the queue to be sent to all remote machines with this connection type.
STATUS, Queued	The total number of status messages that are currently in the queue to be sent to all remote machines with this connection type.
Remote Machine Statistics	
Machine Name	The name of each remote machine with this connection type.
MESSAGES, Sent	The number of messages that the local machine sent to the remote machine.
MESSAGES, Received	The number of messages that the local machine received from the remote machine.
UPDATES, Out	The number of updates that the local machine sent to the remote machine.
UPDATES, In	The number of updates that the local machine received from the remote machine.
TRNSFR SESS, Prime	The number of transfer sessions that occurred during prime time.
TRNSFR SESS, Non-Prime	The number of transfer sessions that occurred before or after prime time.
% USAGE, Prime	The percentage of time that the machine used the network during prime time. The system calculates this percentage by: (1) multiplying the number of prime time hours by the number of ports; (2) then dividing the total usage by the result of step 1. (The system determines the total usage from the Remote Messages Daily Traffic report.)
% USAGE, Non-Prime	The percentage of time that the machine used the network before or after prime time. The system uses the same formula for calculating prime and nonprime time usages. However, for this field, it uses nonprime time hours.
MESSAGES, Queued	The number of messages that are currently in the queue to send to the remote machine.
STATUS, Queued	The number of status messages that are currently in the queue to send to the remote machine.

Viewing the Traffic Snapshot Monthly report

About this task

The Traffic Snapshot Monthly report shows all traffic data that occurred on your messaging system during a month. This report shows all incoming and outgoing traffic for local machines and remote machines.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Server Reports** section, click **Measurements**.
4. In the **Type** field, click **Traffic-Snapshot**.
5. In the **Cycle** field, click **Monthly**.
6. In the **Start Date** field, enter a month in the mm/yyyy format.

   If you do not enter a month, the system uses the current month.
7. Click **Get Report**.
8. In the **Select connection type** field, click a network connection type.
9. Click **Get Report**.

Result

The system displays the Traffic Snapshot Monthly report with the traffic for each remote machine of the connection type you selected.

Traffic Snapshot Monthly report field descriptions

Name	Description
Connection Type	The type of network connection: • Digital = rs232, dcp, or tcp/ip
Start Date	The month of the traffic data; either the month that you entered on the command line or the current month.
Ending Time	The month and day the system stopped collecting data.
TRAFFIC TOTAL	
MESSAGES, Sent	The total number of messages that the local machine sent to all remote machines with this connection type.
MESSAGES, Received	The total number of messages that the local machine received from all remote machines with this connection type.
UPDATES, Out	The total number of updates that the local machine sent to all remote machines (for digital connection types only). Examples of updates are: name, extension, community ID.
UPDATES, In	The total number of updates that the local machine received from all remote machines (for digital connection types only). Examples of updates are: name, extension, community ID.
TRNSFR SESS, Prime	The total number of transfer sessions with this connection type that occurred during prime time.

Table continues…

Name	Description
TRNSFR SESS, Non-Prime	The total number of transfer sessions with this connection type that occurred before or after prime time.
% USAGE, Prime	The total percentage of usage for this connection type that occurred during prime time. This percentage is the sum of all machine usage. (See the % USAGE, Prime field below.)
% USAGE, Non-Prime	The total percentage of usage for this connection type that occurred before or after prime time. This percentage is the sum of all machine usage. (See the % USAGE, Non-P field below.)
Remote Machine Statistics	
Machine Name	The name of each remote machine.
MESSAGES, Sent	The number of messages that the local machine sent to the remote machine.
MESSAGES, Received	The number of messages that the local machine received from the remote machine.
UPDATES, Out	The number of updates that the local machine sent to the remote machine.
UPDATES, In	The number of updates that the local machine received from the remote machine.
TRNSFR SESS, Prime	The number of transfer sessions that occurred during prime time.
TRNSFR SESS, Non-Prime	The number of transfer sessions that occurred before or after prime time.
% USAGE, Prime	The percentage of time that the machine used the network during prime time. The system calculates this percentage by: (1) multiplying the number of prime time hours by the number of ports; and (2) then dividing the total usage by the result of step 1. (The system determines the total usage from the Remote Messages Daily Traffic report.)
% USAGE, Non-Prime	The percentage of time that the machine used the network before or after prime time. The system uses the same formula for calculating prime and nonprime time usages. However, for this field, it uses nonprime time hours.

Interpreting traffic report findings

The various reports can be helpful tools for system planning, diagnosing system and subscriber problems, and for recognizing and diagnosing trends.

Feature Reports and Grade of Service

The Feature Daily Traffic and Feature Hourly Traffic reports each display two separate reports. These reports list session traffic or message traffic information for up to 32 consecutive days or 192 consecutive hours, respectively. The **Maximum Average Voice Ports in Use** field and the **Maximum Average IMAPI Sessions in Use** field are important fields in the Feature Daily Traffic and Feature Hourly Traffic reports.

Important:

These reports play an important role in determining the grade of service (GOS) for the system. Among other uses, GOS is used in determining port requirements. Port requirements on the messaging system are based on the use of ports for all applications, including call answer, messaging, automated attendant, outcalling, and call delivery.

Definition of Grade of Service

GOS is a parameter that describes the delays in accessing a port on the messaging system. Ideally, enough ports must be provided so that a port is always available. However, providing enough ports is not necessary since calls are queued in an automatic call distribution (ACD) group or hunt group until a port is available. This queuing is acceptable to subscribers as long as the delays are not too long.

GOS is defined as the fraction of calls that are queued for longer than 10% of the average holding time on the ports. For example, if the average holding time on an messaging system port is 100 seconds, a 0.05 GOS means that 5% of the calls will experience queueing delays of greater than 10 seconds. A 0.05 or lower GOS is generally recommended for the messaging system.

Determining Grade of Service

To determine the GOS on an installed messaging system, you must retrieve the average number of ports that are used during the busiest hour from the system traffic data. Retrieval can be done by locating the **Maximum Average Ports in Use** field on the Feature Daily Traffic screen. Calculate the average of this value over several days to get a reliable indicator.

Next, locate the number of ports on your system in the first column of the Port Capacity in Erlangs (Avg. Ports in Use) at Various GOS on page 201 table. Look across the row until you find the number that is equal to or just larger than the **Maximum Average Ports in Use** value. The number at the top of the column is the GOS during the busiest hour.

Example of determining Grade of Service

For example, you have a system with 12 ports. Over the course of 5 business days, record the value in the **Maximum Average Ports in Use** field on the Feature Daily Traffic report. Add the five numbers together and divide by five to get an average of 7.25. Look in the Port column in the table for the row that starts with 12, which is the number of ports in this sample system. Looking across that row, note that the value that is equal to or just larger than 7.25 is 7.38. The GOS at the top of the column is 0.05.

You can also use the table to determine the number of ports required for a system under the present load. For example, if a 0.03 GOS is desired, look for the column with the heading of 0.03 GOS. Look down that column to find the number equal to or just larger than the value in the **Maximum Average Ports in Use** field from the Feature Daily Traffic report. Then look across to the value in the left-hand column of that row to determine the number of ports required for a 0.03 GOS.

To continue this example, assume that the **Maximum Average Ports in Use** is 45. In the 0.03 GOS column, the closest value to 45 is 45.38. In the corresponding Port column, you see that 56 ports are required to maintain a 0.03 GOS. Note that ports are always sold in increments of two, so if the number of ports shown is an odd number, round it up by one.

Port Capacity in Erlangs (Avg. Ports in Use) at Various GOS

Ports	0.01 GOS	0.02 GOS	0.03 GOS	0.04 GOS	0.05 GOS	0.06 GOS	0.08 GOS	0.10 GOS
2	0.16	0.23	0.29	0.33	0.38	0.41	0.48	0.54
3	0.47	0.61	0.71	0.79	0.86	0.92	1.03	1.12
4	0.89	1.09	1.22	1.34	1.43	1.51	1.65	1.78
5	1.38	1.64	1.81	1.94	2.07	2.17	2.35	2.49
6	1.92	2.24	2.44	2.60	2.74	2.86	3.06	3.22
7	2.51	2.86	3.11	3.31	3.44	3.58	3.81	4.00
8	3.14	3.53	3.81	4.00	4.17	4.33	4.58	4.78
9	3.78	4.22	4.53	4.75	4.94	5.08	5.36	5.58
10	4.44	4.92	5.25	5.50	5.69	5.89	6.17	6.42
11	5.14	5.67	6.00	6.28	6.50	6.67	6.97	7.25
12	5.83	6.39	6.78	7.06	7.28	7.47	7.81	8.08
13	6.56	7.17	7.56	7.83	8.08	8.31	8.64	8.92
14	7.31	7.92	8.33	8.64	8.92	9.14	9.50	9.78
15	8.03	8.69	9.14	9.47	9.72	9.97	10.33	10.64
16	8.81	9.50	9.94	10.28	10.56	10.81	11.19	11.53
17	9.56	10.29	10.76	11.12	11.41	11.65	12.06	12.39
18	10.34	11.09	11.58	11.95	12.25	12.51	12.93	13.27
19	11.12	11.91	12.41	12.79	13.10	13.37	13.80	14.16
20	11.91	12.72	13.25	13.64	13.96	14.23	14.68	15.05
21	12.71	13.55	14.09	14.49	14.82	15.10	15.56	15.94
22	13.51	14.38	14.93	15.35	15.69	15.98	16.45	16.84
23	14.32	15.21	15.78	16.21	16.56	16.85	17.34	17.73
24	15.14	16.05	16.64	17.08	17.44	17.74	18.23	18.64
25	15.96	16.90	17.50	17.95	18.31	18.62	19.13	19.54
26	16.78	17.75	18.36	18.82	19.20	19.51	20.03	20.45
27	17.61	18.60	19.23	19.70	20.08	20.40	20.93	21.36
28	18.44	19.46	20.10	20.58	20.97	21.30	21.84	22.28
29	19.28	20.32	20.97	21.46	21.86	22.20	22.75	23.19
30	20.12	21.18	21.85	22.35	22.76	23.10	23.66	24.11
31	20.97	22.05	22.73	23.24	23.65	24.00	24.57	25.03
32	21.82	22.92	23.61	24.13	24.55	24.90	25.48	25.95
33	22.67	23.79	24.50	25.02	25.45	25.81	26.40	26.87
34	23.53	24.66	25.38	25.92	26.35	26.72	27.32	27.80
35	24.38	25.54	26.27	26.82	27.26	27.63	28.24	28.72

Table continues…

Ports	0.01 GOS	0.02 GOS	0.03 GOS	0.04 GOS	0.05 GOS	0.06 GOS	0.08 GOS	0.10 GOS
36	25.25	26.42	27.17	27.72	28.17	28.54	29.16	29.66
37	26.11	27.31	28.06	28.63	29.08	29.46	30.08	30.59
38	26.98	28.19	28.96	29.53	29.99	30.38	31.01	31.52
39	27.84	29.08	29.86	30.44	30.90	31.29	31.93	32.45
40	28.72	29.97	30.76	31.34	31.82	32.21	32.86	33.38
41	29.59	30.86	31.66	32.26	32.73	33.13	33.79	34.32
42	30.47	31.76	32.57	33.16	33.65	34.06	34.72	35.25
43	31.35	32.65	33.47	34.08	34.57	34.98	35.65	36.19
44	32.23	33.55	34.38	34.99	35.49	35.91	36.59	37.13
45	33.11	34.45	35.29	35.91	36.41	36.83	37.52	38.07
46	33.99	35.35	36.20	36.83	37.33	37.76	38.45	39.01
47	34.88	36.25	37.11	37.75	38.26	38.69	39.39	39.96
48	35.77	37.16	38.02	38.67	39.19	39.62	40.33	40.90
49	36.66	38.06	38.94	39.59	40.11	40.55	41.27	41.84
50	37.55	38.97	39.85	40.51	41.04	41.48	42.21	42.79
51	38.44	39.88	40.77	41.44	41.97	42.42	43.15	43.73
52	39.33	40.79	41.69	42.36	42.90	43.35	44.09	44.68
53	40.23	41.70	42.61	43.29	43.83	44.29	45.03	45.63
54	41.13	42.61	43.53	44.22	44.77	45.23	45.98	46.58
55	42.03	43.52	44.45	45.15	45.70	46.17	46.92	47.53
56	42.93	44.44	45.38	46.08	46.64	47.10	47.86	48.48
57	43.83	45.35	46.30	47.01	47.57	48.04	48.81	49.43
58	44.73	46.27	47.23	47.94	48.51	48.98	49.76	50.38
59	45.64	47.19	48.16	48.87	49.44	49.92	50.70	51.33
60	46.54	48.11	49.09	49.81	50.38	50.86	51.65	52.28
61	47.45	49.03	50.01	50.74	51.32	51.81	52.60	53.24
62	48.36	49.95	50.94	51.67	52.26	52.75	53.55	54.19
63	49.27	50.87	51.87	52.61	53.20	53.70	54.50	55.15
64	50.18	51.79	52.80	53.55	54.14	54.64	55.45	56.10
65	51.09	52.72	53.73	54.48	55.09	55.59	56.40	57.06
66	52.00	53.65	54.67	55.42	56.03	56.54	57.35	58.01
67	52.91	54.57	55.61	56.37	56.97	57.48	58.31	58.97
68	53.83	55.50	56.54	57.31	57.92	58.43	59.26	59.93
69	54.75	56.43	57.48	58.25	58.86	59.38	60.21	60.88
70	55.66	57.36	58.41	59.19	59.81	60.33	61.17	61.84

Table continues…

Ports	0.01 GOS	0.02 GOS	0.03 GOS	0.04 GOS	0.05 GOS	0.06 GOS	0.08 GOS	0.10 GOS
71	56.58	58.29	59.35	60.13	60.75	61.28	62.12	62.80
72	57.50	59.22	60.29	61.07	61.70	62.23	63.08	63.76
73	58.42	60.15	61.22	62.01	62.65	63.18	64.04	64.72
74	59.34	61.08	62.16	62.96	63.60	64.13	64.99	65.68
75	60.26	62.02	63.10	63.91	64.55	65.08	65.95	66.64
76	61.18	62.95	64.04	64.85	65.50	66.03	66.91	67.61
77	62.10	63.88	64.99	65.80	66.44	66.99	67.87	68.57
78	63.03	64.82	65.92	66.74	67.40	67.94	68.82	69.53
79	63.95	65.75	66.87	67.69	68.35	68.90	69.78	70.49
80	64.88	66.69	67.81	68.64	69.30	69.85	70.74	71.45
81	65.80	67.62	68.76	69.59	70.25	70.80	71.70	72.42
82	66.73	68.56	69.70	70.54	71.20	71.76	72.66	73.38
83	67.66	69.50	70.64	71.48	72.16	72.71	73.62	74.34
84	68.59	70.44	71.59	72.44	73.11	73.67	74.58	75.31
85	69.51	71.38	72.54	73.39	74.06	74.63	75.54	76.28
86	70.44	72.32	73.48	74.33	75.02	75.58	76.51	77.24
87	71.37	73.26	74.43	75.29	75.97	76.54	77.47	78.20
88	72.30	74.20	75.38	76.24	76.93	77.50	78.43	79.17
89	73.23	75.15	76.32	77.19	77.88	78.46	79.39	80.14
90	74.17	76.09	77.27	78.14	78.84	79.42	80.36	81.10
91	75.10	77.03	78.22	79.09	79.79	80.38	81.32	82.07
92	76.03	77.97	79.17	80.05	80.75	81.34	82.28	83.04
93	76.97	78.91	80.12	81.00	81.71	82.30	83.25	84.01
94	77.90	79.86	81.07	81.96	82.67	83.26	84.22	84.97
95	78.84	80.80	82.02	82.91	83.63	84.22	85.18	85.94
96	79.77	81.75	82.97	83.87	84.58	85.18	86.14	86.91

You must monitor port usage regularly and plot it over time to anticipate traffic needs. You must also observe port capacities weekly on new systems or when you are adding new subscribers, and monthly on older systems.

Spotting potential system problems

In addition to helping determine GOS and port usage, the Feature Daily Traffic and Feature Hourly Traffic reports provide statistical information that is useful for spotting potential problems and for evaluating how the messaging system is actually used. This information includes the:

- Number of subscribers administered in the messaging system.
- Total call answer and voice session usage time.
- Number of login attempts and abandoned calls.

- Number of voice mail, call answer, broadcast, login, priority, and private messages sent.
- Average length of voice mail and call answer calls.
- Types of messages, including voice, text, and binary attachments.

Load Reports

The Load Daily Traffic and Load Hourly Traffic reports display information about the number of calls handled by each active port for up to 32 consecutive days or 192 consecutive hours, respectively.

Note:

The **Maximum Simultaneous Ports in Use** field and **Maximum Simultaneous IMAPI Sessions in Use** field in the Load Daily Traffic and Load Hourly Traffic reports provide valuable information about system load, but they are not for use with GOS calculations.

Spotting Switch Problems

The average number and duration of the calls that are made to the messaging system during the period is reported. These numbers could indicate a problem at the switch with either port coverage or distribution if one port is overloaded and other ports are underloaded.

Spotting Threshold Problems

Threshold exceptions indicate that subscribers tried to use more message or list space than was available and that warnings were issued. These exceptions can be the first indication that you need to change certain information contained in other screens.

If you notice a large number of threshold exceptions for lists, it could mean that you initially miscalculated the maximum number of lists per subscriber. You can increase the number of lists assigned to each subscriber through both the Limits and COS screens. You can also ask subscribers to delete old or unnecessary lists.

The upper and lower limits for message space are shown on the screen. If the limits are consistently exceeded, you can do any or all of the following:

- Increase mailbox size for an individual subscriber on the Subscriber screen or for a Class of Service on the COS screen.
- Decrease message retention times on both the Subscriber and COS screens. This action limits the length of time that the messaging system retains messages within subscribers' mailboxes, resulting in the more frequent deletion of old messages.
- Issue a notice (broadcast a message) to subscribers asking them to delete messages immediately after listening to them or to regularly clean both their incoming and outgoing mailboxes.
- Raise the thresholds administered on the Thresholds screen.

Call Management System reports

Avaya Call Management System (CMS) is a product used with the automatic call distribution (ACD) feature of a Communication Manager server. CMS collects call-traffic data, formats management reports, and provides an administrative interface to the ACD feature. CMS also collects data on and provides an administrative interface to the Call Vectoring feature, which is available with the ACD feature on many Avaya switches.

If your company has a CMS connected to your switch and you are using the Call Vectoring feature to route calls to the messaging system, you can use CMS reports to view messaging traffic data.

You can use CMS reports in these circumstances because calls routed to the messaging system through call vectoring are carried on a vector directory number (VDN), which is an extension defined in the switch software. CMS collects data on VDNs and can generate reports on VDNs. Thus, CMS reports on the VDN that carries calls to the messaging system contain traffic data for the system.

The following are examples of the types of messaging data that CMS VDN reports collect:

- The total number of calls to the messaging system.
- The average time that calls waited before being answered by the messaging system if you are using managing split or route to split commands.
- The average length of a call or average talk time to the messaging system.
- The number of calls that transferred out of the messaging system.
- The busiest hour of the day, based on the number of calls.

For more information about CMS and the data you can collect, see the *Avaya Call Management System Administration* and *Avaya CMS Supervisor Reports* documents for your specific CMS release.

Note:

CMS also collects data about the messaging system by identifying the messaging system as a measured ACD split/hunt group. However, measuring a messaging split with CMS is not recommended because messaging split activity can significantly deteriorate the performance of CMS. The messaging split and agent data can also quickly fill CMS disk space.

In addition, CMS VDN data about the messaging system might not match the data collected in messaging traffic reports or ADAP. Calls might spend time in vector processing before actually connecting to the messaging split. CMS collects VDN data on calls during this time, but messaging does not. Additional discrepancies can exist for various reasons, including differing points at which CMS and the messaging system count answered and abandoned calls and the way calls are tracked while being rerouted through the switch.

Security

Overview of Security

This topic describes ways to use system administration tools to minimize the possibility of telecommunications toll fraud on your system. It offers safeguards that make it harder for an unauthorized user to penetrate the messaging system.

What Is Toll Fraud?

Toll fraud is the unauthorized use of a company's telecommunications service. It occurs when people misdirect their own telecommunications charges to another person or business.

For messaging systems, toll fraud consists of using the system and messaging software to complete a toll call through a networked switch.

Note:

Much of the information in this section is from the Avaya Products Security Handbook. See this handbook for complete information on securing your voice mail system from possible toll fraud.

How Toll Fraud Occurs

There are several ways that unauthorized users might attempt to breach your system, including:

- Unauthorized system use
- An intruder accesses your system and creates a mailbox or uses messaging functionality.
- Unauthorized mailbox use
- An intruder discovers how to access a particular mailbox, perhaps by:
  - Finding the password on a subscriber's desk or in a wallet
  - Trying all the common variations of passwords
  - Buying the password from a computer hacker who breached the Linux interface and logged in as an administrator
- Unauthorized use of outcalling call delivery
- Fraudulent call transfer
- An intruder makes use of the transfer to extension (***T**) feature by transferring to the first few digits of a trunk access code.

Unauthorized System Use

To minimize the risk of unauthorized system use, follow the guidelines for your password security, including the Password Aging feature. Provide additional protection for your system with Avaya's Access Security Gateway (ASG) option.

Administration Passwords

The following aspects of password management affect the security of your system:

- Default administrator password
- Password standards
- Password aging

Default Administrator Password

When your system is installed, you will get a default password. You are required to change this password immediately. Use the procedures in Changing Passwords on page 34 to make this change.

Password Standards

Passwords must comply with certain minimum standards. These standards are described in Guidelines for Passwords on page 34.

Password Aging

Password aging ensures that administration passwords are changed at reasonable intervals by causing passwords to expire after a set period of time. Use password aging for administrative logins to reduce the danger of unauthorized system access.

You can specify password aging on the Server (Maintenance) Security Login Account Policy Page. The items and their operation are described in Changing a System Password or Password Aging on page 34.

Access Security Gateway

The Access Security Gateway (ASG) feature is an optional authentication interface that you can use to secure the `craft login` on the Communication Manager server. Whenever a user begins a session on the system for purposes of administration or maintenance, the user must enter a valid login ID. If the ASG interface is activated, the system issues a numerical challenge. In order for the user to access the Communication Manager server and messaging administration and maintenance features, the user must enter the correct numerical response. By activating the ASG feature, you can reduce the possibility of unauthorized remote access to the system.

You administer ASG parameters to specify whether access to the system requires ASG authentication. See the Communication Manager server documentation for appropriate administration and login procedures.

Note:

For more information on using the ASG Key, see the Access Security Gateway Key User's Guide, 585-212-012.

Trusted Server Security

A trusted server is a computer or a software application in a domain outside of messaging. A trusted server uses its own login and password to launch an MCAPI (Message Core Application Programming Interface), LAN session, and access messaging mailboxes.

Trusted servers can access and manipulate a message just as the messaging application can do. See Overview of Activating Internet Messaging on page 285 for in-depth discussions and definitions of trusted servers, domains, and integration of email and other trusted server software with messaging.

Passwords for Trusted Servers

The trusted server can do everything to a user mailbox that a messaging user can do. You must administer a password that the trusted server application uses to request a connection to the messaging server.

The two trusted server screens are MCAPI Options and MCAPI Password. See Activating Internet Messaging on page 285 for trusted server and MCAPI administration information.

To prevent unauthorized access through MCAPI into your system from an external source such as a trusted server, you must administer an MCAPI password that the trusted server uses to connect to messaging. The MCAPI password is another layer of security. It prevents an unauthorized source from starting an MCAPI session.

We recommend that you change MCAPI passwords on a regular basis, for example, monthly. If you set your administrator's password to age automatically, the system prompts you to change your password. You can also use this prompt to remind you to change the MCAPI password.

Virus Detection

Messaging allows the transmission between domains of two message components, text (email) and binary (software) file attachments. When used with a messaging system, (Deprecated) Message Manager also supports these message components. These components introduce the possibility of a computer virus being embedded in a file attachment. While the messaging system cannot be

infected with viruses embedded in these software files, client machines may become infected when a subscriber opens or launches an infected binary file.

Messaging does not perform any virus detection. Your company should carefully evaluate the security risks of file attachments and make provisions for virus detection software on personal computers running an email application or (Deprecated) Message Manager. Your PC/LAN administrator probably has experience in detecting and preventing the transmission of software viruses. Your PC/LAN administrator may also know the minimum requirements that the messaging server and email server must meet to be allowed on the company network at all.

At a minimum, you should advise your subscribers that file attachments should be detached (not launched) and scanned for viruses before use.

Unauthorized Use of Mailboxes

One type of voice mail fraud occurs when an unauthorized user obtains the mailbox password and changes both it and the greeting. The unauthorized user then uses the mailbox for nonbusiness purposes. This use can be expensive if access is gained to the voice mail system through a 1-800 or 1-888 number.

Mailbox Administration

When you administer the system and subscribers' mailboxes, perform the following tasks to prevent unauthorized use:

- To block break-in attempts, administer your system so that the allowed number of consecutive unsuccessful attempts to log in to a mailbox is low. Administer this number on the Administer System Attributes and Features page (Under Messaging Administration, select System Administration).
- Deactivate unassigned mailboxes. When an employee leaves the company, remove the subscriber profile and, if necessary, reassign the mailbox.
- Do not create mailboxes before they are needed.
- Require passwords to be long. The minimum required length is at least one digit greater than the number of digits in subscribers' extension numbers. Subscribers can have passwords of up to 15 digits for maximum security.
- Force subscribers to change the default password the first time they log in to the messaging system. Changing the default password ensures that only the subscriber has access to his or her mailbox, not someone else who enters a subscriber's extension number and then enters #. To ensure that new subscribers change their passwords immediately, administer the default password to be fewer digits than the minimum password length.
- Administer password aging on the **Subscriber Password Aging Limits** > **System Administration** web page. Password aging requires subscribers to change their password at a predefined interval. Password aging enhances overall system security and helps protect against toll fraud by making the messaging system less vulnerable to break-ins.

Subscriber Password Security

To minimize the risk of unauthorized access to messaging mailboxes, ensure that your subscribers follow these guidelines for messaging passwords:

- Never have a personal greeting state that the called extension will accept collect calls or third-party billed calls. If people at your company have this kind of greeting, require that they change the greeting immediately.

- Never use obvious or trivial passwords, such as a room number, employee identification number, social security number, or easily guessed numeric combinations.

  Note:

  The current release of messaging does not allow passwords that consist of sequential numbers such as 12345, repeated numbers such as 33333, and the subscriber's extension number.

- Discourage the practice of writing down passwords, storing them, or sharing them with others. If a subscriber insists on writing down a password, advise the subscriber to keep the password in a secure place and never discard it while it is active.
- Never program passwords onto telephone auto dial buttons.
- If a subscriber receives any suspicious messages or tells you that her or his personal greeting was changed, or if for any other reason you suspect that your messaging system is being used by someone else, contact Avaya Corporate Computer and Network Security, which is described in Avaya Toll Fraud Crisis Intervention on page 264.

Fraudulent Transfers

Once users transfer to dial tone, they can dial a trunk access code (TAC), feature access code (FAC), or extension number. If the system is not properly secured, thieves can make fraudulent long distance calls or request a company employee to transfer them to a long distance number.

Fraudulent transfers can be minimized by administering features and options in messaging and on the Communication Manager server.

Administering messaging to prevent fraudulent transfers

To minimize the risk of fraudulent transfers, you can administer the messaging system with Enhanced Call Transfer and controlled call transfers out of messaging.

Enhanced Call Transfer

About this task

With Enhanced Call Transfer, the messaging system uses a digital control link message to initiate the transfer, and the Communication Manager server verifies that the requested destination is a valid station in the dial plan. With Enhanced Call Transfer, when messaging callers press *** 8** followed by digits (or *** 2** for name addressing) and *****, the system does the following:

Procedure

1. The messaging system verifies that the entered digits contain the same number of digits as the number of digits that are administered on the messaging system for extension lengths.
2. If you restrict call transfers so that calls can be transferred only to administered subscribers, the messaging system also verifies that the digits entered match the extension number for an administered subscriber.

   Note:

   When callers request a name addressing transfer, the name must match the name of a messaging subscriber (either local or remote) whose extension number is in the dial plan.

3. If Step 1 on page 251 is successful, the messaging system sends a transfer control message that contains the digits to the Communication Manager server.
4. If Step 1 on page 251 is unsuccessful, the messaging system plays an error message and asks the caller to try again.
5. The Communication Manager server verifies that the entered digits match a valid extension in the dial plan.
6. If Step 3 on page 251 is successful, the Communication Manager server completes the transfer, disconnects the messaging voice port, and sends a "successful transfer" control link message to the messaging system.
7. If Step 3 on page 251 is unsuccessful, the Communication Manager server leaves the messaging voice port connected to the call and sends a "fail" control link message to the messaging system.

   Then the messaging system plays an error message and asks the caller to try again.

Controlled Transfer Out of Messaging

Most unauthorized long distance call attempts occur as a caller tries to transfer out of the messaging system.

You can control call transfers out of messaging by administering the system to limit the numbers to which a caller can transfer.

Allowed Numbers Menu

To transfer out of the messaging system, the user presses *** T**, the digits of the extension to which she or he wants to transfer, and #. If the pattern of the number dialed corresponds to a pattern that you have permitted on the Allowed Numbers menu, the messaging system initiates the transfer. The Communication Manager server then verifies that it is allowed to transfer to the requested destination.

Before you enable a transfer out of the messaging system, you need to restrict such transfers as described under Controlling Call Transfers on page 67. Within this menu system, you can specify extensions to which a caller can transfer.

Denied Numbers Menu

Callers cannot transfer to extensions that are expressly denied on the Denied Numbers menu. You can, for example, prohibit call transfer to extensions beginning with "9" if dialing this number results in access to an outside line.

If a caller enters an extension that is an allowed transfer, the Communication Manager server completes the transfer, disconnects the messaging system, and sends a "disconnect successful transfer" message to the system. If the number is notan allowed transfer, the Communication Manager server leaves the system connected to the caller and sends a "fail" message to the messaging system. Then the system plays an error message requesting further activity.

Transfer Restrictions

If Call Transfer is activated on the Administer System Attributes and Features page (Under Messaging Administration, select System Administration), you have administered your system to

allow *** T** transfers. You can minimize the risk of toll fraud attempts that use *** T** transfers by taking one or both of the following precautions:

- Setting **the Transfer Restriction** field on the **Call Transfer Out of Messaging** > **System Administration** web page to **subscribers**.
- Administering allowed and denied numbers as described under Controlling Call Transfers on page 67. In this case, if the pattern of the number dialed corresponds to a pattern that you have permitted on the Transfer Security menu system, and if that number is a valid extension number for an administered subscriber (either local or remote), transfer is permitted.

The **Transfer Restriction** field also can be set to **digits**. In this case, the destination telephone number must correspond to a pattern you have permitted and administered in the Transfer Security menu system. It must also have the same number of digits as extension numbers (that is, mailbox identifiers) within the messaging system. Since this option does not minimize toll fraud, it is administered only by Avaya and only as a special service to customers who want the digits option.

Setting the **Transfer Restriction** field to **subscribers** is the more secure of the two options. It virtually eliminates the fraudulent use of call transfer since the messaging system can verify that the specified destination is an administered number. If digits are specified, on the other hand, the caller might find a way to access the Communication Manager server and to use Communication Manager server features and functions to complete fraudulent long distance calls.

Warning:

If you want to assign nonresident subscribers(that is, users with a mailbox but no telephone on the Communication Manager server) to extension numbers that start with the same digit or digits as Communication Manager server trunk access codes (such as 9), you must carefully administer the restrictions by using the Transfer Restrictions menu.

Automated Attendant Security

Automated attendants are used by many companies to augment or replace a switchboard operator. When an automated attendant answers, the caller is generally given several options. A typical greeting is: "Hello, you've reached XYZ Bank. Please press 1 for Auto Loans, 2 for Home Mortgages. If you know the number of the person you are calling, please enter that number now."

If the system is not properly configured, the automated attendant passes the call back to the PBX. The PBX reacts to the digit 9 as a request for a dial tone. The digits 180 become the first numbers of a 1809 call to the Dominican Republic. The 011 string is treated as the first digits of an international call. The hacker then enters the remaining digits of the telephone number and the call is completed. This scenario works the same way with a voice mail system.

Before you set up an automated attendant, restrict transfer out of the messaging system as described in Controlling Call Transfers on page 67.

Administering the Communication Manager server to Prevent Fraudulent Transfers

To minimize the risk of unauthorized persons using the voice messaging or automated attendant systems to make toll calls, administer the voice ports on your Communication Manager server in any of the following ways.

Assign a Low Facilities Restriction Level (FRL)

The Communication Manager server treats all the PBX ports used by voice mail systems as stations. Therefore, each voice mail port can be assigned a COR or COS with a facilities restriction level (FRL) associated with the COR or COS. FRLs provide eight different levels of restrictions for automatic alternate routing (AAR), automatic route selection (ARS), or world class routing (WCR) calls. They are used in combination with calling permissions and routing patterns and/or preferences to determine where calls can be made. FRLs range from 0 to 7, with each number representing a different level of restriction (or no restrictions at all).

The FRL is used for the AAR, ARS, or WCR feature to determine call access to an outgoing trunk group. Outgoing call routing is determined by a comparison of the FRLs in the AAR or ARS routing pattern to the FRL associated with the COR or COS of the call originator.

The higher the FRL number, the greater the calling privileges. For example, when voice mail ports are assigned to a COR with an FRL of 0, outside calls are disallowed. If that is too restrictive, the voice mail ports can be assigned to a COR with an FRL that is higher, yet low enough to limit calls to the calling area needed.

Note:

Voice messaging ports that are outward restricted through COR cannot use AAR or ARS trunks. Therefore, the FRL level does not matter since FRLs are not checked.

FRLs can be assigned to offer a range of calling areas. Choose the one that provides the most restricted calling area that is required. The following table provides suggested FRL values.

Suggested Values for FRLs

FRL	Suggested Value
0	Permit no outgoing (offswitch) calls.
1	Allow local calls only. Deny 0+ and 1800 calls.
2	Allow local calls, 0+, and 1800 calls.
3	Allow local calls plus calls on FX and WATS trunks.
4	Allow calls within the home NPA.
5	Allow calls to certain destinations within the continental United States of America.
6	Allow calls throughout the continental United States of America.
7	Allow international calling. Assign attendant console FRL 7. Note, however, that if Extension Number Portability is used, the originating endpoint is assigned FRL 7.

Note:

FRLs 1 through 7 include the capabilities of the lower FRLs. For example, FRL 3 allows private network trunk calls and local calls in addition to FX and WATS trunk calls.

Setting FRLs

Procedure

1. Use **change cor** for the voice mail ports (versus subscribers) to display the Class of Restriction screen.
2. Enter the FRL number (0 through 7) in the FRL field.

   Assign the lowest FRL that meets the outcalling requirements. The route patterns for restricted calling areas must have a higher FRL assigned to the trunk groups.
3. Use **change route-pattern** to display the Route Pattern screen.
4. Use a separate partition group for ARS on the outcalling ports and limit the numbers that can be called.

   Note:

   The Restricted Call List on the Toll Analysis Table can also be used to restrict calls to specified areas.

Restrict Toll Areas

About this task

A reverse strategy to preventing calls is to allow outbound calls only to certain numbers. You can specify the area code or telephone number of calls you allow.

Procedure

1. Use **change ars analysis** to display the ARS Analysis screen.
2. Enter the area codes or telephone numbers that you want to allow and assign an available routing pattern to each of them.
3. Use **change route-pattern** to give the pattern preference an FRL that is equal to or lower than the FRL of the voice mail ports.

   Note:

   The Unrestricted Call List (UCL) on the Toll Analysis Table can be used to allow calls to specified numbers through ARS and AAR. The COR for the voice mail ports must show "alltoll" restriction and access to at least one UCL.

Create Restricted Number Lists

The Toll Analysis screen allows you to specify the toll calls that you want to assign to a restricted call list (for example, 900 numbers) or to an unrestricted call list (for example, an outcalling number to a call pager). Call lists can be specified for CO, FX, WATS, TAC, and ARS calls, but not for tie TAC or AAR calls.

Monitoring techniques for detecting voice mail fraud

You can use the following monitoring techniques to help determine if your voice mail system is being used for fraudulent purposes:

- Call Detail Recording (or SMDR)
- Traffic Measurements and Performance
- Automatic Circuit Assurance
- Busy Verification
- Call Traffic Report
- Trunk Group Report
- Traffic Reports

Call Detail Recording

About this task

With Call Detail Recording (CDR) activated for the incoming trunk groups, you can find out details about the calls made into your voice mail ports.

Review CDR reports for the following indications of possible voice messaging abuse:

- Short holding times on any trunk group where voice messaging is the originating endpoint or terminating endpoint
- Calls to international locations not normally used by your business
- Calls to suspicious destinations
- Numerous calls to the same number
- Undefined account codes

Procedure

1. Use change system-parameters feature**s** to display the Features-Related System Parameters screen.
2. Administer the appropriate format to collect the most information.

   The format depends on the capabilities of your CDR analyzing and recording device.
3. Use **change trunk-group** to display the Trunk Group screen.
4. Enter `y` in the **SMDR/CDR Reports** field.

Call Traffic Report

This report provides hourly port usage data and counts the number of calls originated by each port. By tracking normal traffic patterns, you can respond quickly if an unusually high volume of calls appears. Such a high volume might indicate unauthorized use, especially if it occurs after business hours or during weekends.

Traffic data reports are maintained for the last hour and the peak hour.

Trunk Group Report

This report tracks call traffic on trunk groups at hourly intervals. Since trunk traffic is fairly predictable, you can easily establish over time what is normal usage for each trunk group. Use this report to watch for abnormal traffic patterns, such as unusually high offhour loading.

SAT reporting

About this task

Traffic reporting capabilities are built in to and are obtained through the System Access Terminal (SAT). These programs track and record the usage of hardware and software features. The measurements include peg counts, that is, the number of times that ports are accessed, and call duration. Traffic measurements are maintained constantly and are available on demand. However, reports are not archived and should therefore be printed if you want to monitor a history of traffic patterns.

Procedure

1. To record traffic measurements:
   a. Type `change trunk-group n` , where *n* is the trunk group number, to display the Trunk Group screen.
   b. Go to page 3, and In the **Measured** field type `both`, if you have both Basic Call Management System (BCMS) and Call Management System (CMS), `internal` if you have only BCMS, or `external` if you have only CMS.
2. To review the traffic measurements:

   Type `list measurements` followed by a measurement type (`trunk-groups`, `call-rate`, `call-summary`, or `outage-trunk`) and time frame (`hourly` or `summary`).
3. To review performance:

   Type `list performance` followed by a performance type (`summary` or `trunk-group`) and time frame (`yesterday` or `today`).

ARS Measurement Selection

About this task

The ARS Measurement Selection can monitor up to 20 routing patterns (25 for G3) for traffic flow and usage.

Procedure

1. Type `change ars measselection` to choose the routing patterns you want to track.
2. Type `list measurements route-pattern` followed by the time frame (`yesterday`, `today`, or `last-hour`) to review the measurements.

Automatic Circuit Assurance

About this task

This monitoring technique detects a number of calls with short holding times or a single call with a long holding time. Such calls could indicate hacker activity. Long holding times on trunk-to-trunk calls can be a warning sign. The Automatic Circuit Assurance (ACA) feature allows you to set time limit thresholds that define what is considered a short holding time and a long holding time. When a violation occurs, a designated station is visually notified.

When an alarm occurs, determine if the call is still active. If toll fraud is suspected (for example, if a long holding time alarm occurs on a trunk-to-trunk call), you might want to use the busy verification feature (see Busy Verification on page 262 for more information) to monitor the call in progress.

Procedure

1. Use `change system-parameters features` to display the Features-Related System Parameters screen.
2. In the **Automatic Circuit Assurance (ACA) Enabled** field, type `y`.
3. In the **ACA Referral Calls** field, type `local`, `primary`, or `remote`.

   If **primary** is selected, calls can be received from other switches. **Remote** applies if the PBX being administered is a DCS node, perhaps unattended, where ACA referral calls go to an extension or console at another DCS node.
4. type `change trunk group` to display the Trunk Group screen.
5. In the **ACA Assignment** field, type `y`.
6. Establish short and long holding times.

   The defaults are 10 seconds (short holding time) and one hour (long holding time).
7. To review, use `list measurements aca`.

Busy Verification

About this task

When toll fraud is suspected, you can interrupt the call on a specified trunk group and monitor the call in progress. Callers will hear a long tone to indicate the call is being monitored.

Procedure

1. Use **change station** to display the Station screen for the station that will be assigned the Busy Verification button.
2. In the **Feature Button Assignment** field, enter **verify**.
3. To activate the feature, press the **Verify** button and then enter the trunk access code and member number to be monitored.

Traffic Reports

The messaging system tracks traffic data over various time periods. Reviewing these reports on a regular basis helps to establish traffic trends. If increased activity or unusual usage patterns occur, such as heavy call volume on ports assigned to outcalling, they can be investigated immediately. You can also use the messaging Administrator's Log and Activity Log to monitor usage and investigate possible break-in attempts. For more information on running and using reports, see Reports on page 201.

Avaya's Statement of Direction

The telecommunications industry is faced with a significant and growing problem of theft of customer services. To aid in combating these crimes, Avaya intends to strengthen relationships with its customers and its support of law enforcement officials in apprehending and successfully prosecuting those responsible.

No telecommunications system can be entirely free from risk of unauthorized use. However, diligent attention to system management and to security can reduce that risk considerably. Often, a trade-off is required between reduced risk and ease of use and flexibility. Customers who use and administer their systems make this trade-off decision. They know best how to tailor the system to meet their unique needs and are therefore in the best position to protect the system from unauthorized use. Because the customer has ultimate control over the configuration and use of Avaya services and products it purchases, the customer properly bears responsibility for fraudulent uses of those services and products.

To help customers use and manage their systems in light of the trade-off decisions they make and to ensure the greatest security possible, Avaya commits to the following:

- Avaya products and services will offer the widest range of options available in the industry to help customers secure their communications systems in ways consistent with their telecommunications needs.
- Avaya is committed to develop and offer services that, for a fee, reduce or eliminate customer liability for PBX toll fraud, provided that the customer implements prescribed security requirements in its telecommunications systems.
- Avaya's product and service literature, marketing information and contractual documents will address, wherever practical, the security features of our offerings and their limitations, and the responsibility our customers have for preventing fraudulent use of their Avaya products and services.
- Avaya sales and service people will be the best informed in the industry on how to help customers manage their systems securely. In their continuing contacts with customers, they will provide the latest information on how to do that most effectively.
- Avaya will train its sales, installation and maintenance, and technical support people to focus customers on known toll fraud risks; to describe mechanisms that reduce those risks; to discuss the trade-offs between enhanced security and diminished ease of use and flexibility; and to ensure that customers understand their role in the decision-making process and their corresponding financial responsibility for fraudulent use of their telecommunications system.

- Avaya will provide education programs for customers and Avaya employees to keep them apprised of emerging technologies, trends, and options in the area of telecommunications fraud.
- As new fraudulent schemes develop, Avaya will promptly initiate ways to impede those schemes, share our learning with our customers, and work with law enforcement officials to identify and prosecute fraudulent users whenever possible.

Avaya is committed to meeting and exceeding our customers' expectations, and to providing services and products that are easy to use and are of high value. This fundamental principle drives our renewed assault on the fraudulent use by third parties of our customers' communications services and products.

Avaya Security Offerings

Avaya has developed a variety of offerings to assist in maximizing the security of your system. These offerings include:

- Access Security Gateway (ASG) for the Communication Manager server.
- Security Audit Service of your installed systems.
- Fraud Intervention Service.
- Individualized Learning Program, a self-paced text that uses diagrams of system administration screens to help customers design security into their systems. The program also includes a videotape and the Avaya Products Security Handbook.
- A call accounting package that calls you when preset types and thresholds of calls are established (not available on S8300 Server).
- A remote port security device that makes it difficult for computer hackers to access the remote maintenance ports.
- Software that can identify the exact digits that have passed through the voice mail system.

For more information about these services, see the Avaya Products Security Handbook.

Avaya Toll Fraud Crisis Intervention

If you suspect that you are being victimized by toll fraud or theft of service and need technical support or assistance, call one of the following numbers immediately.

Technical Service Center (TSC)	800-242-2121
Technical Service Center Toll Fraud Intervention Hotline	800-643-2353

Note:

These services are available 24 hours a day, 365 days a year. Consultation charges might apply.

Avaya Corporate Security

Whether or not immediate support is required, please report all toll fraud incidents perpetrated on Avaya services to Avaya Corporate Security. In addition to recording the incident, Avaya Corporate

Security is available for consultation on product issues, investigation support, law enforcement, and education programs.

Fax Messaging

Fax messaging allows subscribers to send and print Faxes to telephone numbers of up to 31 digits. It also enables a shortcut key (**5) to print to the machine you specify . To print all new faxes, from the main menu, press `74`. You control what Fax numbers subscribers can call by allowing or denying dial strings. Fax Messaging works with the messaging software telephone interface and with (Deprecated) Message Manager Release 4.6 and later.

Fax messaging is enabled by default, and the default Fax server name is "Fax", and cannot be changed.

Intended use

Communication Manager Messaging is not intended to provide the functionality of a Fax server. For example, the messaging software does not support attempts to send Fax documents to lists comprised of hundreds of recipients.

Fax machines

The Fax feature testing made use of emulation tools to test the interoperability of the Fax feature with a broad representative sampling of Fax machines. The testing indicates that the Fax feature can be expected to be interoperable with most Fax machines. Due to the large number of models and brands of Fax machines, there might be some models that do not interoperate well with the Communication Manager Messaging Fax feature.

T.38 IP Fax Signaling Protocol

The SIP Integration supports receipt of incoming Fax messages on all channels simultaneously. Support for Fax with SIP VoIP integrations is based on the T.38 Fax signaling protocol and is dependant upon Communication Manager for support of the T.38 protocol. Fax messaging is *only* available with SIP integration.

The T.38 Fax provides support of a-law encoded transmissions over an IP trunk. This support is needed in a network environment where the calls are shuffled over a network path not necessarily including the switch hop, which may be encoded in a-law and not converted to u-law.

Fax dependencies on outcalling

Outcalling does not have to be turned on for Fax to work, but the outcalling period and ports are used by Fax for printing.

You cannot directly administer the netcycle for a Fax machine. You must administer outcalling which is the global setting for the netcycle of each network device. The netcycle for a Fax machine is 24 hours. The netcycle range is from 0.00 hours to 23:59 hours. So, if the system outcalling period was set from 18:00 hours to 20:00 hours, then a Fax print issued outside the period will not be printed until 18:00 hours. If you re-administer the outcalling period, it will take 24 hours for any existing Faxes to print at the new time.

The number of outcalling ports impacts the number of print jobs that can be finished during the outcall period.

The outcalling period and ports are set in the Outcalling Options page (Select **Messaging Administration** > **Outcalling Options**).

Fax capacities

You must refer to your Communication Manager server documentation to determine your maximum Fax capacity. The availability of your Communication Manager resources determines the maximum number of simultaneous Faxes that can be sent. For more information about your Communication Manager resources, see Communication Manager and Call Center System Software Based Capacities, 03-300511.

Your Fax capacity is the maximum number of Faxes that you can send or receive. Factors such as call traffic and the dynamics of resource allocation can lower your Fax capacity. If you experience routine problems with your Fax capacity limits, you might have to upgrade some of your Communication Manager hardware or software.

For example, if you had a G350 media gateway, you would have 32 resources available. With no shuffling, each Fax you send over an IP trunk configured for T.38 requires 8 resources, 4 for the T.38 segment used internally for the messaging software and 4 for the T.38 segment on the IP trunk. The system maximum would be 4 Faxes, assuming no other call traffic on the system.

IP trunk configuration

Fax calls that use more than one IP segment, and have a configuration that prevents call shuffling, might have time-out issues with some Fax messages. Fax call failures are more likely to occur as the complexity of the call path and switch network increases. For more information, see Avaya FoIP, MoIP & TTYoIP.

Checklist for administering Fax Messaging

The following table outlines the procedures required to administer Fax Messaging:

Process	Procedure to Use
Set system Fax options.	Setting System Fax Options on page 266
Specifying Fax Dial Strings.	Specifying Fax Dial Strings on page 267
Enabling FAX Messaging on an Individual Basis (if needed).	Enabling Fax Messaging on an Individual Basis on page 269
Enabling FAX Messaging by Defining a Class of Service (COS).	Enabling FAX Messaging by Defining a COS on page 270
Notify subscribers of Fax capability.	Administering Avaya (Deprecated) Message Manager for FAX Messaging on page 275
Maintenance and Administration.	Maintenance and Administration on page 276

Setting System Fax Options

About this task

To enable the messaging software to use Fax Messaging:

Procedure

1. Go to the Communication Manager Messaging System Management Interface web page.
2. Click **Administration** > **Messaging**.

3. Under **Messaging Administration** , click **Fax Options**.
4. Verify that the **Fax Enabled?** field is set to **Yes**.

   Note:

   Fax is the default name of the Fax server and cannot be changed.
5. In the **Fax Deliveries to the Specified Dial Strings** field, select **Allowed** or **Denied**, whichever is appropriate.
6. For more information about the values in this field and about allowing or denying numbers, see Specifying Fax Dial Strings on page 267.
7. Click **Update Features** to save the information in the system database.

Listing Fax Dial Strings

About this task

A Fax dial string specifies the digits at the beginning of a telephone number. The Fax dial strings administered on the system determine which telephone numbers subscribers can use when addressing or printing Faxes. To display a list of all the Fax dial strings currently entered in the system:

Procedure

1. Go to the Communication Manager MessagingSystem Management Interface web page.
2. Click **Administration** > **Messaging**.
3. Under **Messaging Administration**, select **Fax Dial Strings**.

   The system displays the dial strings added in the Messaging system.
4. The system adds the word Allowed or Denied to the screen title as an indication of whether you entered allowed or denied in the **Fax Deliveries to All the Specified Dial Strings Are Allowed/Denied** field on the Fax Options page.

   If you specified **Allowed**, then the Fax Dial Strings page lists all the dial strings that subscribers can use when addressing or printing Faxes.

   If you specified **Denied**, then the Fax Dial Strings page lists the dial strings that subscribers are not allowed to use when addressing or printing Faxes.

   Note:

   If you specified **Denied** and no dial strings are listed, then subscribers can address Faxes to any telephone number.

Specifying Fax Dial Strings

About this task

A Fax dial string specifies the digits at the beginning of a telephone number. The system allows up to 200 Fax dial strings. You have three choices for controlling telephone numbers to which outgoing Faxes can be sent or printed.

Procedure

1. To allow subscribers to send or print Faxes to any telephone number:
   a. On the Fax Options page; choose **Denied**.
   b. On the Fax Dial String page:

      Do not specify any dial strings.
2. To allow subscribers to send or print Faxes to any telephone number except for the numbers you want to deny access:
   a. On the Fax Options page, choose: **Denied**.
   b. On Fax Dial String page:

      Specify dial strings that begin telephone numbers that subscribers cannot use.
3. To allow subscribers to send or print Faxes to only specific telephone numbers:
   a. On the Fax Options page, choose: **Allowed**.
   b. Specify only the dial strings that begin telephone numbers that subscribers can use for sending or printing Faxes.

Adding Fax Dial Strings

Procedure

1. Determine which specific Fax dial string you want to allow or deny.

   The Fax dial string must include the trunk access code and applicable access, country, or area codes.
2. For example, 901157 is a dial string that consists of:
   - 9, the trunk access code
   - 011, the international dialing code
   - 57, the country code
3. Go to the Communication Manager Messaging System Management Interface web page.
4. Click **Administration** > **Messaging**.
5. Under **Messaging Administration**, select **Fax Dial Strings**.
6. On the Fax Dial Strings page, click **Add String** button.

   For example, type nnnn, where nnnn is the dial string to be added. The dial string can contain up to 31 digits, and the digits can be from 0 through 9. Spaces, star (*), or pound (#) are not allowed.
7. The system displays a text box to add the fax dial string.

   If you specified **Allowed** on the Fax Options page, then the Fax Dial String page specifies that the dial string will be allowed, which means that subscribers can use the specified dial string when addressing or printing Faxes.

If you specified **Denied** on the Fax Dial String page, then the Fax Dial String page specifies that the dial string will be denied, which means that subscribers cannot use the specified dial string when addressing or printing Faxes.

8. Click **Add String**.

Removing Fax Dial Strings

About this task

As the needs of subscribers change, you can remove dial strings that were previously allowed or denied. Also, before you can change the allowed or denied setting in the **Fax Deliveries to All the Specified Dial Strings Are Allowed/Denied:** field on the Fax Options page, you must remove all existing Fax dial strings. To remove one or all Fax dial strings:

Procedure

1. Go to the Communication Manager Messaging System Management Interface web page.
2. Click **Administration** > **Messaging**.
3. Under **Messaging Administration**, select **Fax Dial Strings**.
4. From the Fax Dial Strings page, determine Fax dial string that you want to remove.
5. Select the dial string and click the **Delete String** button.
6. **(Optional)** You can also choose to delete all the listed strings by using the **Delete All Strings** button.

Administering Subscribers for FAX Messaging

Fax capabilities can be administered:

- On an individual, subscriber-by-subscriber basis
- For a Class of Service (COS)
- As a separate, secondary Fax extension for those subscribers who send and receive a greater than average number of Fax messages

This section tells you how to perform these three tasks.

Enabling FAX Messaging on an Individual Basis

About this task

Once you have administered FAX Messaging on the messaging software, you are ready to enable your subscribers so that they can use this feature.

Note:

If you change an individual subscriber's COS, you remove any association between the subscriber and any other class of service. Therefore, if you have administered or are planning to administer a special COS for FAX Messaging, do not use this procedure. Instead, follow the procedure Enabling FAX Messaging by Defining a COS on page 270.

To enable a subscriber for FAX Messaging:

Procedure

1. Go to the Communication Manager Messaging web page.
2. Click **Administration** > **Messaging**.
3. Under **Messaging Administration**, select **Subscriber Management**.
4. Click **Manage** to view the list of local subscribers.
5. Select a subscriber.
6. Click **Edit / Delete the Selected Subscriber**.

   The system displays the Edit the Local Subscriber page.
7. On the Edit the Local Subscriber page, under **PERMISSIONS** do the following:
   a. Use the Tab key to move to the **Fax Creation?** field (under **)**.
   b. Select **Yes** in the field.
8. Under **MISCELLANEOUS**, in the **Voice Mail Message Maximum Length** field, enter the larger number of the following two choices:
   - A value that is double that of the current voice-only capacity (for example, change a maximum message length of 700 seconds to 1400 seconds)
   - At least 1200 seconds (20 minutes)
9. In the **Call Answer Message Maximum Length** field, enter a value of at least 1200 seconds.
10. In the **Mailbox Size** field, enter the larger number of the following two choices:
    - A value that is double that of the **Voice Mail Message Maximum Length** you entered in Step 6 (for example, if the value just entered was 1400 seconds, set **Mailbox Size:** to 2800 seconds)
    - At least 2400 seconds (40 minutes) of capacity
11. Click **Save** to update this information to the system database.

Note:

Enabling a subscriber for FAX Messaging has no effect unless FAX Messaging is enabled for the Communication Manager Messaging system. For more information, see Setting System Fax Options on page 266.

Enabling FAX Messaging by Defining a COS

About this task

To enable FAX Messaging for a class of service (COS)

Procedure

1. Go to the Communication Manager Messaging web page.
2. Click **Administration** > **Messaging**.

3. Under **Messaging Administration**, select **Classes-of-Service**.
4. Select the Class-of-Service in which you want to enable FAX messaging.
5. Click the **Edit the Selected COS** button.
6. Under **PERMISSIONS**, in the **Fax Creation?** field, select **yes**.
7. Under **MISCELLANEOUS**, in the **Voice Mail Message Maximum Length** field, enter a value of at least 1200 seconds.
8. In the **Call Answer Message Maximum Length** field, enter a value of least 1200 seconds.
9. In the **Mailbox Size** field, enter a value of least 2400 seconds.

   This value is double that of the value in the **Voice Mail Message Maximum Length** field.
10. To update the information to the system database, click **Save**.

Note:

Enabling a subscriber for FAX Messaging has no effect unless FAX Messaging is enabled for the Communication Manager Messaging system. For more information, see Setting System Fax Options on page 266.

Administering a Secondary Fax Extension

About this task

Subscribers who receive a large number of Faxes can have a separate, secondary extension dedicated to incoming Fax calls. Voice messages cannot be recorded at this extension, nor can other subscribers address messages to it.

To administer a secondary Fax extension on the system, you set up a second, Fax-dedicated extension for a subscriber's mailbox. The subscriber then has two extensions and one mailbox. The primary extension is administered for Call Answer, Personal Greetings, and other voice mail services. The secondary Fax extension provides only a brief greeting that reveals the subscriber's name and invites the caller to leave a Fax.

To administer a secondary Fax extension:

Before you begin

1. Have the switch administrator create a phantom extension with a Direct Inward Dialing (DID) number for the subject subscriber. Note the extension number created.
2. Have the switch administrator administer the phantom extension to cover directly to the messaging software. This way, the secondary Fax extension can be dialed as if it were a Fax machine.

Procedure

1. Go to the Communication Manager Messaging System Management Interface web page.
2. Click **Administration** > **Messaging**.
3. In **Messaging Administration**, select **Subscriber Management**.
4. To view the list of local subscribers, click **Manage** .

5. Select a subscriber, and click **Edit / Delete the Selected Subscriber** .

   The system displays the Edit the Local Subscriber page.

6. Under **Basic Information** do the following:

   a. Use the Tab key to move to the **Secondary Ext** field.

   b. Type the secondary Fax extension number of the subscriber.

   Note:

   This number must have the same number of digits as the primary extension.

7. To update the information in the database, click **Save**.

Administering Guaranteed Fax

Guaranteed Fax provides coverage for busy or out-of-service Fax print destination machines, such as a stand-alone Fax machine or a Fax modem on a PC. If the Fax print destination machine is unavailable, Guaranteed Fax redirects the Fax to a mailbox for temporary storage. This Guaranteed Fax mailbox is set to autoprint back to the originally called Fax print destination machine.

Guaranteed Fax Considerations

The interaction of the Fax print destination machine's extension and the Guaranteed Fax mailbox requires periodic monitoring. There are several considerations that you need to take into account when implementing and maintaining this mailbox:

- The Guaranteed Fax mailbox must be large enough to temporarily store a potentially large number of Fax files.
- The Guaranteed Fax mailbox is designed to accept Faxes only from remote messaging systems or Fax machines. It must not be implemented when all traffic is from one messaging system.
- Faxes that have somehow not been removed by autodelete must be manually deleted periodically; otherwise, the mailbox could be filled to maximum capacity.
- The mailbox must be periodically monitored for voice, file attachments, and e-mail messages. These come into the mailbox as part of a voice/Fax/e-mail message, but they are never removed by autodelete.
- The Fax machine's paper supply and toner cartridge must be periodically monitored. If the Fax machine is out of paper, the Guaranteed Fax mailbox will fill up with Faxes that cannot be printed.
- Do not leave auto print turned on for an out of service Fax machine. If you leave auto print on, you can fill the mailbox with cover sheets from every unsuccessful attempt to print a Fax.

Choosing a Guaranteed Fax Administration Type

Guaranteed Fax is typically administered as a secondary extension, but it can also be administered as an ordinary subscriber. Each method has its advantages. In either case, the Fax endpoint is set up on the switch for call coverage to the messaging software so that, if the Fax print destination machine is busy, an incoming Fax is directed to the messaging mailbox.

When Guaranteed Fax is administered as a secondary Fax extension, the mailbox is treated as a printer. Voice, file attachments, and e-mail components of an incoming call are ignored. The Fax data is recorded and the Fax print destination machine is tried repeatedly until the Fax can be

delivered. No other messaging features are available on a secondary Fax extension. See Administering Guaranteed Fax as a Secondary Extension on page 273 for procedural information.

When Guaranteed Fax is administered as an ordinary subscriber, the Fax print destination machine is treated as a messaging extension. The messaging software can be used with this number exactly as it can be used for any messaging subscriber. For example, a Fax can be sent directly to the Fax print destination machine's extension as a message to a messaging extension. On the other hand, voice messages sent to this mailbox (perhaps as attachments to forwarded Fax messages) remain in the mailbox and use a portion of the total mailbox size. You must manually delete such messages. See Administering Guaranteed Fax as a Communication Manager Messaging Subscriber on page 274 for procedural information.

Administering Guaranteed Fax as a Secondary Extension

About this task

To administer a Fax endpoint as a secondary Fax extension:

Before you begin

1. Have your switch administrator add a phantom extension number. The number must be within the range of numbers in the messaging dial plan, but it cannot be an extension number that is recognized by the switch.
2. Have the switch administrator administer the Fax print destination machine's extension for call coverage to messaging.

Procedure

1. Go to the Communication Manager Messaging web page.
2. Click **Administration** > **Messaging**.
3. Under **Messaging Administration**, select **Subscriber Management**.

   The system displays the Manage Subscribers page.
4. In the **Add or Edit** text box, type a new subscribers extension.

   The system displays the Add Local Subscriber page. See, adding a messaging subscriber as described in Adding Subscribers on page 94.
5. Enter the Fax print destination machine's extension number as a secondary extension as described in Administering a Secondary Fax Extension on page 271.
6. Use the telephone interface to:
   - Record the name of the Fax print destination machine. When the system prompts you for your name, reply with the name of the Fax machine, for example, "Sales department Fax machine."
   - Record a greeting that identifies the Fax print destination machine.
   - Enter the Fax endpoint extension as the default Fax print destination machine. This value must match the allowed or denied Fax dial string restrictions as described in Specifying Fax Dial Strings on page 267.
   - Activate **Autoprinting** from the mailbox (to the specified endpoint).
   - Activate **Autodelete** to help keep the mailbox from exceeding maximum storage.

Administering Guaranteed Fax as A Communication Manager Messaging Subscriber

About this task

To administer a Fax endpoint as a messaging subscriber:

Procedure

1. Have the switch administrator administer the Fax machine's extension for call coverage to messaging.
2. Go to the Communication Manager Messaging web page.
3. Click **Administration** > **Messaging**.
4. Under **Messaging Administration**, select **Subscriber Management**.

   The system displays the Manage Subscribers page.
5. In the **Add or Edit** text box, type in a new subscribers extension.

   The system displays the Add Local Subscriber page. See, adding a messaging subscriber as described in Adding Subscribers on page 94.
6. Under Incoming Mailbox, in the **Retention Times** field, enter a value of 3 or 4 days.

   Keep this value low to avoid accumulating undeleted messages. However, you must also consider what the longest period of time is that the destination Fax machine will go unattended, for example, over a 4-day holiday weekend.
7. Under MISCELLANEOUS, in the **Call Answer Message Maximum Length** field, enter `1200` seconds.
8. In the **Mailbox Size** field, enter a minimum value of seconds.

   Note:

   5000 seconds is the equivalent of 50 to 150 pages of Fax, depending on the nature of the Fax. Monitor this setting to ensure that its value is sufficient to guarantee storage of all incoming Faxes. If this mailbox is heavily used or regularly receives graphic-intensive Faxes, you might need to increase the mailbox size (to 10,000 seconds, for example).
9. To update the information to the system database, click **Save**.
10. Use the telephone interface to:
    - Record the name of the Fax print destination machine. When the system prompts you for your name, reply with the name of the Fax machine, for example, "Sales department Fax machine."
    - Record a greeting that identifies the Fax print destination machine.
    - Activate **Autoprinting** from the mailbox (to the specified Fax endpoint).
    - Enter the Fax print destination machine extension as the default Fax machine. This value must match the allowed or denied Fax dial string restrictions as described in Specifying Fax Dial Strings on page 267.

- Activate **Autodelete** to delete Fax messages after a successful autoprint.

Administering Avaya (Deprecated) Message Manager for FAX Messaging

The specific steps for administering (Deprecated) Message Manager for FAX Messaging are detailed in the Message Manager on page 323 section. However, for FAX Messaging to run on (Deprecated) Message Manager, you must:

- Enable FAX Messaging for the messaging software.
- Enable your (Deprecated) Message Manager users for FAX Messaging.
- Install the Fax version of (Deprecated) Message Manager Release 4.0 or later.
- Administer Communication Manager Messaging for Messaging Application Interface Program (MCAPI) by using the **MCAPI Options** link under Messaging Administration.

Informing Subscribers of Fax Messaging Capabilities

Once FAX Messaging is set up, subscribers need information about how to create and address Fax messages. You can cut and paste this information into a message to your users or add it to an internal Web site.

Creating a Fax Message from a Fax Machine

About this task

You can create a Fax message by accessing your messaging mailbox from a Fax machine and then scanning the document you want to Fax:

Procedure

1. Use the handset of the Fax machine and log in to your messaging mailbox.
2. When prompted, press **1**(Create a Message) on the telephone keypad of the Fax machine.
3. When prompted, press **#**(To send only a Fax).
4. When prompted, begin addressing:
   - For extensions on the local system, enter the extension number and #.
   - For numbers outside the local PBX:
     - Press ****5**.
     - Enter the Fax number as a subscriber would dial it from an internal desk phone, including the trunk access code and the long distance access codes.
     - Press **#**.
   - For messaging mailing lists, press ***L** and follow system prompts.
5. After you have finished addressing, press **#**.
6. Listen for voice prompts to instruct you to load the document.

   Then press **Start** on the Fax machine.

Creating a Fax Message by Forwarding from Your Mailbox

About this task

You can forward a Fax message from your messaging mailbox. You can get the Fax into your mailbox either by sending a Fax to your messaging mailbox from a Fax machine or by receiving a Fax from someone else.

Procedure

1. Send a Fax to your own mailbox or receive a Fax from someone else.
2. Log in to your messaging mailbox.
3. When prompted, press **2**(Get Messages) on the telephone keypad.
4. When you hear the header for the Fax message, press 0 to listen.
5. Press **1**(Respond to or forward message).
6. Press **2**(Forward with comment).
7. Record the voice comment and then press **#**.
8. When prompted, begin addressing:
   - For extensions on the local system, enter the extension number and #.
   - For numbers outside the local PBX:
     - Press ****5**.
     - Enter the Fax number as a subscriber would dial it from an internal desk phone, including the trunk access code and the long distance access codes.
     - Press **#**.
   - For messaging mailing lists, press ***L** and follow system prompts.
9. After you have finished addressing the message, press **#**.

Maintenance and Administration

Important:

Performing ongoing administration and preventive maintenance is the key to problem-free system operation. It is important to establish a regular schedule for maintenance tasks. Performing regular administration and maintenance identifies problems that could otherwise be compounded.

This section addresses the following information:

- Checking the Administrator's Log
- Checking the Alarm Log
- Monitoring Guaranteed Fax
- Checking Message Delivery Increments (Retry Schedule)
- Monitoring Usage of Mailbox Space

Checking the Administrator's Log

About this task

Access the Administrator's Log screen to view current messages and a description of administrative events. Some of these events, such as full subscriber mailboxes and undeliverable messages, directly affect Fax processing.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **Logs** section, click **Administrator**.

   The system displays the Administrator's Log screen.
4. Click **Display**.
5. Examine the displayed events.

   For information about events, alarms, and their associated repair procedures, see *Communication Manager Messaging Events, Alarms and Errors Reference*.
6. To display messaging platform events, do the following:
   a. Repeat Step 2 and 3.
   b. In the **Application** field, type `VP`, and click **Display**.

Checking the Alarm Log

About this task

The alarm log contains descriptions of all significant problems detected by the system. The alarm log contains active alarms and resolved alarms (that is, alarms that were corrected either automatically or by repair procedures). You must check the alarm log regularly.

To view the alarm log:

Procedure

1. Log on to Communication Manager MessagingSystem Management Interface.
2. Select **Administration** > **Messaging**.
3. Select **Logs** > **Alarm** .
4. In the **Alarm Type** field, select **Active** or **Resolved**.
5. To display a specific alarm level, select **yes** in the corresponding alarm level field:

   Major, Minor, and/or Warning.
6. To display alarms for a date other than the current date, in the **Start Date** field, enter that date in the **mm/dd/yy** format.

7. To display alarms for a specific time period going forward, in the **Time** field, select the beginning time in the **hh/mm** format.
8. If you want to select specific alarms, select the resource type, the application, and/or the alarm code
9. Click **Display** to display the alarms.
10. Examine the displayed events.

    A list of events and alarms and associated repair procedures is included in *Communication Manager Messaging Events, Alarms and Errors Reference*. Take whatever corrective action is necessary to repair the alarm.

Monitoring Guaranteed Fax

Several routine maintenance tasks are required to ensure smooth operation of Guaranteed Fax, including:

- Checking that the Fax machine is operational
- Monitoring the space available in the mailbox associated with the guaranteed Fax extension
- Removing any accumulated voice, file attachments, and e-mail messages

Checking that the Fax Machine Is Operational

When you administer a Fax machine for guaranteed Fax, ensure that someone is responsible for the operation of the machine. Have that person check the Fax machine daily to ensure that it is not:

- Turned off
- Broken
- Out of paper
- In need of toner
- Jammed

Monitoring and deleting messages

About this task

The system makes regular attempts to delete voice messages, file attachments, and e-mail messages and to regulate Fax message storage in these mailboxes. However, messages can occasionally be retained. Therefore, you must regularly check Guaranteed Fax mailboxes for voice messages, file attachments, and e-mail messages as well as undeliverable Fax messages.

Procedure

1. Access the mailbox through the telephone interface and access message headers by pressing **2** on the telephone keypad.
2. Delete each voice message by using the *** 3** command on the telephone keypad.
3. Also on the telephone keypad, press **4** at the Activity menu to access the outgoing mailbox of the guaranteed Fax print destination machine.

Press *** #** to step through the message categories to listen for the category of undeliverable messages. (These are messages that can remain undeliverable, for example, because of some temporary problem with the Fax machine).

4. If you know the Fax machine is currently working, step through the message headers by pressing either **# #** to resend the messages or *** 3** to delete the messages, as appropriate.

   Continue until there are no more undeliverable messages.

5. Press *** * 9** to exit the telephone interface.

Checking Message Delivery Increments (Retry Schedule)

About this task

A message that is directed to a Fax print destination machine could fail if the Fax machine is in use, turned off, out of paper, or broken. Fax call delivery could also fail if the receiving machine or subscribers on the receiving machine are not Fax enabled. The system makes six attempts to deliver a Fax before the message fails.

To specify how often delivery attempts are made:

Procedure

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

   The system displays the Administer System Attributes and Features page.

4. To reschedule the intervals for which the call delivery messages, including outbound Fax messages, use **Rescheduling Increments for Full Mailbox Delivery**.

   Only the first five increments apply to Fax deliveries. After six unsuccessful tries, a Fax is considered undeliverable.

5. To change the rescheduling increments, go to the Increment field that you want to change, and enter a different value.
6. To update this information to the system database, click **Save**.

Monitoring Usage of Mailbox Space

About this task

During the first few weeks of FAX Messaging operation, subscribers might tell you that the messaging system often reports that their mailboxes are full. If such reports are frequent for a particular subscriber, consider expanding the capacity of the subscriber's mailbox.

Note:

If a subscriber receives a partial Fax, verify if the subscriber's mailbox is full. If there is not enough room in the mailbox to accept the entire Fax, the message is truncated. If the mailbox is not full when the subscriber receives a partial Fax, the subscriber's maximum call answer

message size might be too small to contain the message. The system administrator can check "admin.log" to see if subscriber's mailboxes are full.

To monitor usage of mailbox space:

Procedure

1. Go to Communication Manager Messaging System Management Interface.
2. Select **Administration** > **Messaging**.
3. Select **Server Reports** > **Measurements**.
4. In the **Type** field, select **Subscriber**, and in the **Cycle** field select **Daily**.
5. Click **Get Report**.
6. Provide the extension of the subscriber whose mailbox you want to check.

   The system displays Measurements page;Subscriber Daily Traffic Report with information that pertains to the current date.
7. Compare the number of seconds in the **Mailbox Space Used** field with the administered value in the adjacent **Space Allowed** field.

   If these two fields are roughly equivalent, you need to increase the mailbox size as described in Enabling FAX Messaging on an Individual Basis on page 269.

   To increase mailbox size for a COS, follow the procedure Enabling FAX Messaging by Defining a COS on page 270.

Email (Internet Messaging)

Internet Messaging Concepts and Planning

Internet Messaging Features

Internet Messaging has the following characteristics:

Internet Gateway	Messaging subscribers gain an Internet email address and can send or receive messages over the Internet. Internet Messaging uses Extended Simple Mail Transport Protocol (ESMTP), a standard TCP/IP-based mail protocol.
Mailbox access through POP3 or IMAP4 clients	In addition to the telephone user interface (TUI) and (Deprecated) Message Manager 4.3 and greater, subscribers can also select one of the currently available POP3 or IMAP4 email client programs to check their messages. For example, Netscape Mail or Microsoft Outlook can be used to receive and respond to messages through the messaging software.

What Internet Messaging Can Do for You

Internet Messaging can:

- Provide access for messaging subscribers to any of the email users worldwide through the Internet.
- Increase the number of choices that subscribers have to access messages, including telephone, (Deprecated) Message Manager, and industry-standard email platforms.
- Save costs by allowing message transport through existing, shared Internet facilities.

Sending and Receiving Email

Internet Messaging gives (Deprecated) Message Manager and Post Office Protocol 3 (POP3) or Internet Message Access Protocol 4 (IMAP4) client subscribers full Internet email capabilities through the messaging. Multimedia messages can be sent from the messaging software to any email address. The recipients can access these messages as multi-part MIME messages using commercially-available email software. Voice components are played with the G711 wave format through your PC.

Email Access With Computer Applications

The following access methods are available:

- (Deprecated) Message Manager subscribers can send and receive all four component types to and from Internet email users, as with any other messaging destination. These component types include voice, fax, text, and file attachments.
- POP3 and IMAP4 client subscribers can use their browser to access their messaging mailboxes. Voice components are played with the G711 wave format. Graphics programs display fax files. Text and attached files are handled as with any other email.
- Non-messaging users access messages using the same message-rendering tools as POP3 or IMAP4 client subscribers, except the messages are delivered through their own Internet service provider.

Email access through the telephone

With Internet Messaging for messaging, subscribers can use the telephone to manage messages received at their messaging mailbox. The message waiting indicator (MWI, such as the indicator lamp or a stutter dial tone) is activated to alert a subscriber to the arrival of new messages.

The message can contain up to four media types, specifically voice, fax, text, and file attachments. From the telephone, subscribers can:

- Receive an email message that can contain up to four media type components.
- Listen to a voiced rendering of the text component (if the messaging Text-to-Speech feature is activated).
- Print the text and/or fax component of an email message to a fax machine.
- Reply to an email message, whether it came from a messaging subscriber or an Internet email address.

A message is treated as a single entity when accessed via a telephone. When subscribers play a message that contains a voice, a fax, a text, and a file attachment component, they hear the following:

- Voice component
- A voiced summary of the fax component and instructions on how to print the fax
- The spoken text-to-speech output of the text component (if enabled)
- A voiced summary about the attached file

Optional Email Features

Two features provide additional access to message information:

- Text-to-Speech (TTS) conversion is an optional feature that enables subscribers to listen to a voiced rendering of email and (Deprecated) Message Manager text messages received in their messaging mailboxes.
- Message components are rendered as follows:
  - The subject line of an email message is read as part of the message header.
  - The body of the text message is voiced.
  - If a file attachment is included in the email message, that component is not voiced. The subscriber hears summary information regarding the size of the file.
  - Fax components are also summarized regarding the number of pages contained in the fax.
- Text-to-Fax (TTF) enables subscribers to print the text and/or fax component of an email message to a printer or fax machine. For the text component, the messaging software uses the Text-to-Fax feature to translate the component into printed form.
- Messages are printed in plain text, without formatting and special attributes such as bold type or tab settings.

Planning

Before you install Internet Messaging, you must consider the email size, LAN impact, subscriber planning, and security issues.

Email Message Size

Email messaging can have a significant impact on the size set for a subscriber's mailbox. An email message can be a short memo or can include attachments of software files of considerable size. If subscribers send fax and voice messages, planning is more difficult.

Messaging converts all message components into seconds of space in the mailbox.The following tables show some examples of typical mailbox sizes and corresponding maximum email and maximum message length capacities.

Mailbox Suggested Sizes and Maximum

Mailbox Size, in seconds and (hours:minutes)	Mailbox Size, in MB	Notes
2400 sec (0:40 hr)	19.2 MB	The message size is determined by multiplying the message length in seconds by 8000 and dividing by 1000000.
3600 sec (1:00 hr)	28.8 MB	
4800 sec (1:20 hr)	38.4 MB	
8400 sec (2:20 hr)	67.2 MB	System default
32767 sec (9:06 hr)	262 MB	System maximum for one subscriber's mailbox

Email and Voice Message Sizes, Suggested Sizes and Maximum

Message Length, in seconds and (minutes)	Message Size, in MB	Notes
600 sec (10 min)	4.8 MB	The message size is determined by multiplying the message length in seconds by 8000 and dividing by 1000000.
900 sec (15 min)	7.2 MB	
1200 sec (20 min)	9.6 MB	System default
10800 sec (180 min or 3 hours)	86.4 MB	System maximum for one message

LAN Impact

Use the following table to estimate how much of the LAN traffic on the system will be comprised of email messages (including email with attached components).

LAN Impact of Email Messaging

Component	Size
Voice	60 seconds = 480 1-KB packets
Fax	3 pages = 145 1-KB packets
Email	5 KB = 5.5 1-KB packets
Attachments, including email attachments	around 150 KB (file size varies by type of file and contents)

Subscriber Planning

Prepare subscribers by taking the following steps:

- Inform users about their messaging email capabilities. See Notifying Subscribers of Email Capability and Setup on page 294 for more information.

- Allow (Deprecated) Message Manager subscribers to add email addresses to their personal address books or their messaging lists to simplify addressing.
- Determine whether to allow messaging subscribers to access messages in their messaging mailbox with a POP3 or IMAP4 email program. The messaging software can send messages similar to any mail gateway, but allowing this access presents certain security risks. See Security Issues on page 284 for more information.
- When questions arise, or in the initial training about messaging email, describe the following differences to subscribers:
  - When a message is sent from a messaging subscriber to recipients in both messaging and the Internet, the messaging recipients are not listed on the Internet recipient's email To: list. Therefore, the email recipients do not know which messaging subscribers also received the message and cannot use the email application's Reply All function to send a reply to the messaging recipients of the original message.
  - Messages expire within a time period determined by the subscriber or COS mailbox settings. Subscribers need to understand this difference because email accounts do not usually have this limitation.
  - Users can set their email application (such as Outlook or Exchange) to forward mail automatically to another email address or to their messaging email address. messaging does not allow mail to be automatically forwarded to another email address.

Security Issues

Security alert:

Toll fraud is the theft of long distance service. When toll fraud occurs, your company is responsible for charges. See Overview of Security on page 251 for information on how to prevent toll fraud, or call the Avaya Technologies National Customer Care Center at 1-800-643-2353.

Using Internet Messaging and the Internet presents certain security issues. Your company is responsible for any damages that could arise as a result of the use of Internet Messaging. However, you can administer your system to minimize these risks. You need to be concerned with:

Disabling POP3 or IMAP4 Access

On the Messaging SMI System Adminstration page, if the **POP3 port** or **IMAP4 port** fields are set to **Enabled**, hackers could determine a subscriber's login name and password, and then commit toll fraud through the subscriber's mailbox. Use Internet Messaging only behind a corporate firewall and restrict external Internet access to the appropriate email client ports.

If your company is concerned with subscriber login security, consider the following alternatives:

- Disable the POP3 or IMAP4 interface by selecting **Disabled** on the System Administration page and enable the **IMAP4 SSL** or **POP3 SSL** port.
- Exclusively use email clients such as Qualcomm's Eudora client that support password encryption.
- Deploy secure socket layer (SSL) for POP3 or IMAP4 using an external SSL accelerator.

Viruses

The ease with which messages can be broadcast and transmitted over the Internet simplifies the distribution of computer viruses. Enact a policy to ensure that subscribers check incoming messages and files for viruses.

Another precaution, especially important if this is your company's first email deployment, is a system-wide virus scanning application. The applications scan all incoming mail for viruses and intercept infected mail and files before they get to the subscriber.

Spoofing or Sending Email Under a False Name

Internet email addresses are not validated for identity. As a result, the identity of the message sender is not guaranteed. Warn your subscribers not to respond to messages from unverified sources, especially if the message contains requests for private information or any form of payment. The name of the machine that delivered a message to the Internet Messaging server can be checked by reading the message's header information.

Internet Messaging for Communication Manager Messaging builds on the multimedia capabilities of messaging to provide exchange of voice, fax, text, and binary components over the Internet.

Activating Internet Messaging

Overview of Activating Internet Messaging

Important:

There are important issues to consider before beginning to activate the Internet Messaging feature. Check the Planning on page 282 and Security on page 280 sections and confirm that these issues have been addressed.

The Internet Messaging feature is already installed with Communication Manager Messaging. However, a number of steps are required to have the feature work properly for your network and subscribers, including administering the Internet Messaging screens and making sure that the feature is working properly. After these steps are completed, subscribers can send and receive messages.

This topic describes information to gather and procedures to complete for the activation process.

Administering Internet Messaging

About this task

Administration changes on the Internet Messaging screens are required so that the system operates properly in your location. After becoming familiar with the operation of Internet Messaging and the type of traffic your subscribers generate, you can use these screens to improve the management of the feature's operation.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging**.
3. In the **IMAP/SMTP Administration** section, click **General Options**.

   The system displays the General Options and Settings screen.

Note:

Internet Messaging places default values in many fields to simplify initial setup. As usage patterns become clear, you can adjust the fields that have defaults to the most appropriate value.

4. Check the contents of each field for the correct entry. Leave the values on this screen unchanged unless the traffic volume, subscriber requests, or other system requirements dictate otherwise.
5. If you want to allow the POP3 or IMAP4 users to use the system directory as their email directory, go to the System Administration web page and select the appropriate client and port options.

   Security alert:

   If you enable POP3 or IMAP4 message access, password integrity may be compromised during each login. Therefore, Avaya recommends that you administer the access for use only behind a corporate firewall, and that you disable mailbox access from outside the firewall. If you enable POP3 or IMAP4, Avaya is not responsible for any theft of service that might occur. See Security on page 280 for more information.
6. In the **IMAP/SMTP Administration** section, click **Mail Options**

   The system displays the Mail Options screen.
7. Select the appropriate options and then click **Save**.

   Use the **Help** button for additional information about the available settings.

Testing the Operation of Internet Messaging

About this task

After the messaging software and Internet Messaging are administered, run the following tests to confirm that all network connections are established and that the system is operating properly.

Procedure

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

   The system displays the Internet Messaging: IMAP/SMTP Status page.
4. Verify that the **Internet Message status** is **Running**.

   Note:

   For an explanation of how to run the test or of the test results, click the **Help** button at the bottom of each Internet Messaging screen.
5. In the left navigation pane, under the **Diagnostics** group, click **Name Server Lookup**.

The system displays the Test Name Server Lookup page.

6. Run the Name Server Lookup test for the messaging software and mail gateway.

   Test each host name or IP address. Use the name format of hostname domain. For example, use the name messaging.dr.avaya.com, not just *messaging*.

7. This test determines whether a system can be looked up through the domain name servers assigned on the TCP/IP Networking screen.

   If domains can be looked up, messages can be delivered to them.

8. In the left navigation pane, under the **Diagnostics** group, **SMTP Connection**.

   The system displays the Internet Messaging: SMTP Connection Test page.

9. In the **IP Address or Host Name** field, an IP address or fully qualified internet host name.

10. Click **Run Test**.

    Run test for each host name or IP address. This test validates the mail protocol connection between this messaging system and another machine.

11. In the left navigation pane, under the **Diagnostics** group, perform one of the following:

    - Click **POP3 Connection**.
    - Click **IMAP4 Connection**.

12. In the **IP Address or Host Name** field, an IP address or fully qualified internet host name.

    Test each host name or IP address. This test calls a network host using TCP/IP to determine whether the host's POP3 or IMAP4 interface is running.

13. In the left navigation pane, under the **Diagnostics**, click **Mail Delivery**.

    The system displays the **Internet Messaging: Mail Delivery Test** page.

14. Run the Mail Delivery test for a known messaging extension and password, and a valid email address.

    This test validates whether the mail system is functioning by sending a message through the messaging system to an existing extension.

15. Go to the extension and verify that the test message was delivered.

16. In the left navigation pane, under the **Logs** group, click **IMAP/SMTP Messaging**.

17. The system displays the Internet Messaging Logs page.

18. Check each log for the messaging status in each delivery process.

    You can select the log you want to view from Logs.

Internet Directory

Configuring the Internet Directory Feature

When Internet Messaging is purchased, the default for LDAP is ON. You must enable LDAP for the Internet Directory feature to work. You can enable this feature as needed.

When LDAP is ON, the Internet Directory is created and populated with the names, email addresses, and extension numbers of local messaging subscribers as listed on the Subscriber screen.

The Internet Directory is located on the message server and is automatically updated whenever subscriber names, email addresses, or extensions are changed.

Verifying the LDAP status

Procedure

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

   The system displays the Administer System Attributes and Features page.
4. Verify the settings for the **LDAP port** and the **LDAP SSL port** fields.

   LDAP is enabled when the fields are set to **Enabled**, and LDAP is disabled when the fields are set to **Disabled**.
5. Verify the settings in the **Anonymous LDAP Authentication** field.

   If the **Anonymous LDAP Authentication** field is set to `Authenticated or Anonymous`, anonymous binds are permitted. Anonymous binds are useful for integrating with standards-based email clients for directory lookup.

Administration

The Internet Directory feature requires no separate administration. When you add, change, and delete subscribers on the Subscriber screen the Internet Directory is automatically updated to reflect any changes to the name, extension, and email address. You cannot directly modify the Internet Directory.

The Internet Directory is accessed from the LDAP interface that is on the messaging server. If you cannot access the Internet Directory after configuring one of the email products for LDAP, contact your certified Avaya service representative.

Note:

If the email field on the messaging Subscriber Screen is blank, the email field in the Internet Directory is also blank. This field does not display the messaging Internet Messaging address based on the extension. You will need to update the email address field on the Subscriber screen to include this address in the Internet Directory.

If the messaging server's domain name is changed, the system administrator must manually change the email address in the Subscriber screen, or the Internet Directory will not reflect the change.

Accessing the Internet Directory

The Internet Directory is located on the message server. External clients can use the following to access the Internet Directory.

- Microsoft Outlook 97 or later, Internet Mail version only
- Microsoft Outlook Express
- Mozilla Thunderbird
- Netscape Messenger with Netscape Communicator, 4.5 or later
- Eudora Pro, 4.1 or later

System administrators will need to inform outside email users about how to access the messaging Internet Directory. Before the directory can be accessed, the following information must be configured in LDAP directory properties for the email program on the client workstation:

- Client-created descriptive name for the Internet Directory
- Messaging server address, for example, **messageserver1.YOURcompany.com**
- Search options set as **dc=Avaya**
- Port number set as **389**

The procedures required for users to add this directory to their email service are different for each of the email products. Below are some general procedures, but this information is subject to change. The email users need to be told to review the online Help associated with their email service for instructions about how to set up a new LDAP directory service.

Checking the Alarm Log

About this task

Errors that occur in the Internet Directory are sent to the messaging alarm log. The alarm log contains descriptions of all significant problems that have been detected by the system. The alarm log contains active alarms and resolved alarms; that is, alarms that are corrected either automatically or manually by repair procedures. The system administrator must check this log on a daily basis.

To check the alarm log for Internet Directory problems:

Procedure

1. Follow the steps in Reports on page 201 to access alarm information.
2. To display Internet Messaging specific alarm information, leave all fields at their default setting, except the following:
   - If you want to display an alarm for a date other than the current date, enter that date (in the format mm/dd/yy), in the **Start Date** field.
   - **Alarm Code**Enter `6617`, the code for an LDAP failure.
3. Click **Display**.

   The alarm log is displayed.

4. Examine the displayed alarms.

   Verify if alarm code 6617 is listed under the heading **Alarm Code**. Alarms, events, and their associated repair procedures are described in *Communication Manager Messaging Events, Alarms and Errors Reference*.

Result

The Internet Directory feature is available with the Communication Manager Messaging, Internet Messaging feature. This feature enables the messaging software to create an Internet directory with subscriber names, email addresses, and extensions from the messaging subscriber information. External email clients can use their LDAP directory server to reference these email addresses and extensions.

LDAP stands for Lightweight Directory Access Protocol. LDAP has become the standard for Internet-based applications to use for access to directory information.

This section provides information for the Internet Directory feature only. It does not provide the procedures that you need to administer the Internet Messaging feature, or to plan for its implementation. See Overview of Activating Internet Messaging on page 285 for details on administering Internet Messaging and Internet Messaging Concepts on page 280 for details on planning for Internet Messaging.

Email Administration

Overview

Internet Messaging is an optional application that provides email capabilities for Communication Manager Messaging. Topics in this section include:

- Enabling Email
- Enabling Email by Defining a COS
- Defining Remote Email Users
- Retaining Non-administered Remote Email User Information
- Notifying Subscribers of Email Capability and Setup
- Preventive Maintenance and Troubleshooting

Before you continue

This section describes only a portion of the tasks needed to administer Internet Messaging. See the Email (Internet Messaging) on page 280 section for a list of tasks for performing messaging email installation and administration. You must perform the tasks in the Activating Internet Messaging on page 285 section prior to performing the administration described in this section.

Designing a multimedia messaging system involves solid planning. You should involve your PC/LAN system administrator and your email administrator in this planning phase. See Internet Messaging (Concepts and Planning) on page 280 for more information.

Enabling email

There are two ways to enable subscribers for email:

- On an individual, subscriber-by-subscriber basis
- By defining a Class of Service (COS)

Enabling Email on an Individual Basis

About this task

If you change an individual subscriber's COS profile fields on **Edit a Class-of-Service** page, you remove any association between the subscriber and any other Class of Service options you may set up in the future. If only a few subscribers need email access, you can enable each subscriber individually, as described in this procedure.

Note:

The following procedure contains instructions relating only to the one or two fields on a particular screen that you must administer. See Subscriber Administration on page 91 for complete field descriptions.

To administer an individual subscriber for email:

Procedure

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

   The system then displays the Manage Subscribers page.
4. In the Local Subscriber row, click **Manage**.

   The system displays the Manage Local Subscribers page.
5.
6. Select a subscriber you want to administer and click **Edit/Delete the Selected Subscriber**.
7. The system displays the Edit Local Subscriber page.
8. Under the **Permissions** section, in the **MCAPI Access**, select **yes**.
9. In the **MCAPI Message Transfer** field, select **yes**.
10. Check the **Voice Mail Message (seconds), Maximum Length** field.

    The system default is 300 seconds. (This size is sufficient to contain a 9.6 MB email message. See Planning on page 282 for other suggested values.)
11. Check the **Mailbox Size (seconds), Maximum** field.

    The system default is 2100 seconds. (This size provides 67.2 MB for storage of the subscriber's voice, fax, text (email) and binary attachments. See Internet Messaging Planning on page 280 for other suggested values.)
12. Click **Save** to update the information in the system database.

    Ensure that your subscribers have sufficient training and instructional material to take full advantage of this additional functionality. See Notifying Subscribers of Email Capability and Setup on page 294 for guidelines and more information.

Result

This subscriber's mailbox is now enabled for email integration.

Enabling Email by Defining a COS

About this task

If you have a large number of subscribers to administer, defining a COS takes less time than administering subscribers individually.

Note:

The following procedure contains instructions relating only to the one or two fields on a particular screen that you must administer. See Subscriber Administration on page 91 for complete field descriptions.

To administer predefined groups of subscribers for email:

Procedure

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

   The system then displays the Manage Classes-of-Service page.
4. Select a COS you want to administer and click **Edit the Selected COS**.

   The system displays the Edit a Class-of-Service page.
5. Under the **Permissions** section, in the **MCAPI Access** field, select **yes**.
6. In the **MCAPI Message Transfer** field, select **yes**.
7. Check the **Voice Mail Message (seconds), Maximum Length** field.

   The system default is 300 seconds. (This size is sufficient to contain a 9.6 MB email message. See Internet Messaging Planning on page 280 for other suggested values.)
8. Check the **Mailbox Size (seconds), Maximum** field.

   The system default is 2100 seconds. (This size provides 67.2 MB for storage of each subscriber's voice, fax, text (email) and binary attachments. See Internet Messaging Planning on page 280 for other suggested values.)
9. Click **Save**, to update the information in the system database.

   Ensure that your subscribers have sufficient training and instructional material to take full advantage of this additional functionality. See Notifying Subscribers of Email Capability and Setup on page 294 for guidelines and more information.

Note:

If, after time, you find that your system disk space is running low, consider purchasing additional mailboxes or disk space.

As an alternative to purchasing more disk space, you might consider reducing the number of days that messages are retained in subscribers' mailboxes. To do so, change the values in the **Retention Time** fields. Make this change only after careful consideration, and give subscribers advance notice.

All subscribers of this COS are now enabled for email integration.

Defining Remote Email Users

About this task

If your subscribers will be frequently sending messages to email users, you can permanently define the email addresses of those email recipients in the local messaging software. This way, your subscribers can address messages to these email users using their telephones, and can add them to their personal directories.

Before starting this procedure, you need to know the name of the trusted server to which the remote user is to be added, and the proper format for the email address.

To see a listing of all trusted servers on your system, select **Trusted Servers** under **Server Administration**.

To see the proper format for email addresses on that server, select **Remote Text Addresses** under **Server Reports**.

To define a remote email user to the messaging software:

Procedure

1. Go to the **Messaging Administration** main menu and select under **Messaging Administration**:

   Subscriber Management

2. The system displays the Manage Subscribers page.
3. Click **Manage** for a Remote Machine.
4. Click the Add a remote Subscriber button.
5. The system displays the Add a Remote Subscriber page.
6. Type the email user's name in the **Subscriber Name** field and press the TAB key.

   Note:

   The name of any remote-subscriber that contains an embedded space, such as the name **Jane Doe**, must be put in quotation marks, that is **"Jane Doe"**.

7. Enter the remote text address for the email system in the proper format (for example, username@machine.domain) in the **Text Address** field and press the TAB key.

Note:

Your email administrator should be able to give you this address.

8. If you are using community IDs to define sending communities, enter the 1-digit to 15-digit number in the **Community ID** field and press the TAB key. This ID number should match that of the trusted server.

   For information on sending communities, see Setting Up Community Sending Restrictions on page 72.

9. Click Save to update the information in the system database.

Retaining Non-administered Remote Email User Information

About this task

A messaging email user can send a message to a messaging mailbox as long as the message is addressed to the messaging subscriber's extension. The messaging software receives the message and retains the email address of the non-administered remote sender. This information is retained by the system for the length of time specified on Non-Admin Remote Subs page.

The advantage of the system retaining this information is that a messaging subscriber who receives a message from a non-administered remote email user can reply to that message without having to re-address it. Messaging software subscribers can also add a non-administered remote email user to mailing lists.

To administer the retention time for non-administered remote email addresses:

Procedure

1. Go to the **Messaging Administration** main menu and select under Messaging Administration:

   Non-Admin Remote Subs

2. The system displays the Non-Administered Remote Subscriber Options page.
3. Complete the fields on this screen using the information in the table for Field Definitions: Non-Administered Remote Subscriber Options page.
4. Click Update Options.

Notifying Subscribers of Email Capability and Setup

About this task

After Internet Messaging is activated, administered, and functioning properly, you can tell your subscribers how to use the new feature. This section contains draft text that you can copy, paste, and modify to create an educational email for your subscribers.

To create an email to notify subscribers of email capability:

Procedure

1. View this documentation file with a web browser.
2. Select and copy the **Courier font** text in this section, starting with Internet Messaging overview on page 295.

3. Click in a blank email message and paste the text.
4. Read the template text and look for text that is written inside the square brackets ([ ]).
5. Decide how you will address the issues marked with square brackets and change the text to meet the needs of your subscribers.

   This text must be changed to include information that is appropriate for your site.
6. Delete any topics that do not apply to your company's communication strategy.
7. Add any information your subscribers might need to use Internet Messaging effectively.
8. Send the email to any subscribers that have email capability.

Internet Messaging overview

You can now send voice messages in an email over the Internet!

Recently, your system administrator installed Internet Messaging for Communication Manager Messaging. This means you can now use the voice mail messaging software to send and receive electronic mail [to and from the Internet]. Internet Messaging works with many commercial email programs. You can also send a voice attachment that the message recipient can hear.

In this message we explain how to:

* address messages from other email programs to the Internet

* address messages from an Internet address to a Communication Manager Messaging mailbox

* configure your POP3 or IMAP4 email program to access a Communication Manager Messaging mailbox

Keep this message so you can refer to the instructions later.

Addressing from (Deprecated) Message Manager to an Internet email address

How do I address a message from (Deprecated) Message Manager to an Internet mail recipient ?

If you know the Internet address of the recipient, you can use this addressing scheme:

handle@host.domain

where "handle" is the person's email name and "host.domain" is the Internet address for their email server. This is the regular email addressing scheme you have used with other email programs.

For example, you could send an email message to John Doe at the Friendly Company at this address:

johndoe@friendly.com

If an internet email user sent you a message, their address is in the "From:" field.

Addressing from another email program through Communication Manager Messaging to an Internet email address

How do I address in my email program through the messaging software to an Internet email address?

You can use any POP3 or IMAP4 compliant email program to access your messages with Communication Manager Messaging. Most commercially-available programs comply with this protocol. Addressing is the same as through other email servers.

If you know the Internet address of the recipient, you can use this addressing scheme:

handle@host.domain

where "handle" is the person's email name and "host.domain" is the Internet address for their email server. For example, you could send an email message to John Doe at the Friendly Company at this address:

johndoe@friendly.com

If an internet email user sent you a message, their address is in the "From:" field.

Addressing from an Internet email address to a Communication Manager Messaging mailbox

How does an Internet email user address messages to my Communication Manager Messaging mailbox?

The email address for your Communication Manager Messaging mailbox is:

extension@[host.domain]

[or the email address administered on the subscriber's form]

"Extension" is your [3 to 50]-digit extension number. [host.domain] is the Internet address of your Communication Manager Messaging server. When you send email from the Communication Manager Messaging system, the system default of first.last@host.domain is used as your return address.

[Two other schemes are available. You can use your first name, a period, your last name, then @[host.domain]. Or, you can use the character "+", then your full phone number using "." or "-" separators, then @[host.domain]. However, the "extension@" form is the primary address for your mailbox.]

Configuring [your company's POP3 email program] to access the Communication Manager Messaging mailbox:

About this task

How do I use [POP3 email program] to access my Communication Manager Messaging mailbox?

Instead of using (Deprecated) Message Manager or the Telephone User Interface (TUI), you can now check your messages using [POP3 email program].

Note:

If [POP3 email program] does not have a "Leave messages on server" option, it is NOT RECOMMENDED for retrieving messages from your Communication Manager Messaging mailbox.

Follow these steps under the [menu option or tab settings, customize for your site's POP3 email program]:

Procedure

1. Change the POP3 user name to [3 to 50]-digit extension [or to extension/nomove, for example 56789/nomove].

   * If user name is extension, each time [POP3 email program] accesses your Communication Manager Messaging mailbox, all "new" messages are moved to the "old" category and the message waiting lamp is turned off.

   *If user name is extension/nomove, new messages remain as "new" (and the message waiting lamp stays on) until the user moves them from the "new" category to "old" or to a personal directory. A user could accomplish such a move by using the telephone user interface (TUI) or (Deprecated) Message Manager.
2. Change the [outgoing mail or SMTP] server to [host.domain].
3. Change the [incoming mail or POP3] server to [host.domain].
4. Select the ["Leave messages on server" or your program's similar] option.
5. Set the "Reply to:

   " or "email address" field to [first.last@host.domain.]
6. Set the ["check for new messages"] to [10 minutes or greater].
7. To retrieve messages, click the ["Get Mail"] option.
8. Enter your Communication Manager Messaging mailbox password at the prompt.
9. Process outgoing and incoming email messages.

Using Internet Messaging

- Voice components of Communication Manager Messaging messages appear as wave file attachments.
- Record an audio component from your computer, then attach the new file to the outgoing message.
- Fax components of Communication Manager Messaging messages appear as .TIF attachments. Use an appropriate graphics viewer to see these components.

Configuring [your company's IMAP4 email program] to access the Communication Manager Messaging mailbox

About this task

How do I use [IMAP4 email program] to access my Communication Manager Messaging mailbox?

Instead of using (Deprecated) Message Manager or the Telephone User Interface (TUI), you can now check your messages using [IMAP4 email program].

Follow these steps under the [menu option or tab settings, customize for your site's IMAP4 email program]:

Procedure

1. Change the IMAP4 user name to [3 to 50]-digit extension.

2. Change the [outgoing mail or SMTP] server to [host.domain].
3. Change the [incoming mail or IMAP4] server to [host.domain].
4. Set the ["Reply to:

   " or "email address" field to first.last@host.domain.]
5. Set the [check for new messages] to [10 minutes or greater].
6. Use "Idle" if it is supported by the client.
7. 7.

   Check your options for [When I delete a message:] under [Server Settings]. Select one of the following options:

   - [- Mark it as deleted]
   - [- Remove it immediately]

   If you select the [Move it to the Trash Folder] option, CMM creates an IMAP4 server-side Trash folder a and deleted messages are moved to that folder.
8. To retrieve messages, click the [Get Mail] option.
9. Enter your Communication Manager Messaging mailbox password at the prompt.
10. Process outgoing and incoming email messages.

Result

The message waiting lamp turns off after the message is read. Messages that are marked for deletion remain in the INBOX folder until they are [purged].

Preventive Maintenance and Troubleshooting

This section describes how to check for system alarms relating to email and how to locate troubleshooting information.

Checking the Alarm Log

About this task

The alarm log contains descriptions of all significant problems detected by the system. The alarm log contains active alarms and resolved alarms; that is, alarms that are corrected either automatically or by repair procedures. This log should be checked on a daily basis.

To check the alarm log for Internet Messaging problems:

Procedure

1. Follow the steps in Reports on page 201 to display the alarm log.
2. Check the **Resource Type** column for Server alarms.

Checking the Trusted-Server Profile

About this task

To check the status of a machine that has generated an alarm or to verify information about a trusted server:

Procedure

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

   The system displays the Manage Trusted Servers page.
4. Click **Display Report of Trusted Servers**.

   The system displays the Report of Trusted Servers page.

Result

Now you can view the profile of the all administered trusted servers.

Troubleshooting Email

The Internet Messaging application contains an extensive troubleshooting section. For troubleshooting information, access the online help from the Internet Messaging web administration pages.

Chapter 6: Data managment

Overview

Purpose of Backup and Restore

It is recommended to back up Messaging data.

The Communication Manager server backs up messaging data over the customer's LAN to an external server. In the event of a system failure, the information stored on the external server is used to restore the system to an operational state.

The system administrator who is administering network backups using FTP, SCP or SFTP, needs to be cognizant of the possible file storage size and any limitation of the storage size on the customer's data network.

The number of mailboxes for the messaging application on an supported platform can be in thousands. Hence, the message storage size on the system server hard disk drive has increased significantly.

Previously, customers may have seen backup file sizes of maybe 100MB or more of data.

With 2,000 or 3,000 or more administered mailboxes the backup files could possibly be more than 10GB of data.

Most IT administrators constrain their data networks to a few GB's of data, so the network backup process may be stopped if the file sizes get too large when using FTP, SFTP or SCP to transfer the backup data from the Communication Manager Messaging Server's hard disk drive to the customer's network FTP, SFTP or SCP server.

A system administrator can mitigate the backup file size by:

- Limiting the mailbox size of users to fewer hours of storage, so that users do not have more than 10 or so minutes of voice storage in their mailbox
- Limiting the number of days a message can remain in a mailbox before the message is deleted. Currently the system defaults to 15 days of shelf life for a message before it is deleted. The system automatically deletes messages with the nightly audits when the messages age to the administered number of days.

Note:

Depending on the severity of the situation, the messaging software might have to be reinstalled before you can restore any backups.

Data that you can back up and restore

You can back up any combination of the four messaging data types at any time manually (Backup Now) or according to a schedule automatically (Scheduled Backup). The four data types are:

- Translations
- Announcements
- Messaging names
- Messaging greetings and messages.

Translations

Translations comprise system administration data.

- Detailed system data on shared memory, speech file system pointers, and so on
- Alarm management information
- A list of enabled features
- A list of installed software
- Messaging Digital Networking connectivity and communication information
- Message headers, mailing lists, subscriber profiles (including automated attendant administration), and message-waiting indicator status
- Switch integration parameters
- Hard disk configuration

In addition to the scheduled backups, you should perform a backup now whenever you make extensive changes to subscriber profiles.

Announcements

Announcements are the prompts and phrases that guide the user through the messaging application. This data type does not require a backup unless the system has customized announcements that have just been changed. If customized announcements are not being used, a backup of announcements already exists on the original factory software CD.

Messaging names

The messaging names data type contains voiced subscriber names. After additional subscriber names have been recorded, you should conduct a backup now of this data type.

Voice messages

Voice messages are all of the call answer and voice mail messages that subscribers send and receive every day. Also included are voice messaging greetings,which include each subscriber's primary voice greeting, multiple personal greetings, automated attendant menus and messages, and bulletin board messages.

Backup now

Use Backup Now when you want to back up system data immediately. For example, you may want to back up data very soon after you have installed the Communication Manager server and/or the messaging system. Additionally, you may want to run the backup procedure just before making a change to your system. Doing so ensures that the most recent data is backed up, including data that is new since the last scheduled backup was run.

Note:

The "backup now" does not cause a degradation in service. However, for best results, perform a backup now at a time when the messaging system experiences low usage.

Additionally, the messaging backup files can be quite large. As a result, your LAN network connection may fail during a backup now. In this case, you can run a scheduled backup instead, which allows the Communication Manager server to handle breaks in the LAN connection and ultimately create a successful backup. To run a scheduled backup in case of a failed backup now, you can simply set the schedule to run on the current day of the week and 5 or 10 minutes in the future. See Create (add) a new backup schedule on page 307.

Scheduled backup

The scheduled backup occurs automatically according to a schedule that you set for the system. The scheduled backup can contain all of the information necessary to bring the messaging system back to an operational state after a service-affecting event.

Scheduled backups do not require supervision. However, for the backup to be successful, you must ensure that the external server to which messaging sends backup data still has space to accept a new backup.

FTP server setup and maintenance

File transfer protocol(FTP) is the Internet protocol standard mechanism for moving files from one machine to another. The FTP backup method requires use of an FTP server, which must be connected to the same enterprise LAN as the Communication Manager server. The customer LAN administrator is responsible for setting up an FTP backup server.

Configure the FTP server

It is recommended that the FTP server be installed and configured before the installation and use of the Communication Manager server and messaging software. The configuration includes creating a directory for storing backups. Since you will normally backup the Communication Manager server and messaging data during the same backup, use the same directory for Communication Manager server and messaging backups. Use a directory name that makes sense and is easy to remember, such as c:\ftp\s8400back.

Disk space on the FTP server

The messaging data can require a lot of disk space. Depending on the number of subscribers, the number of announcement sets you customize, and the amount of message storage you allow, a single full system backup can require 300 MB or more (up to approximately 800MB). This amount of data is in addition to the data backed up for the Communication Manager server itself. Additionally, for each backup, the system creates a new file based on the date and time the backup is run. This means you cannot overwrite a backup previously stored.

As a result, it is recommended that you delete old backup files periodically and diligently, at the same rate at which you perform backups. If the server runs out of disk space for the backup, data will be stored up to the point of failure. Data is stored in the following order of priority: translations, announcements, names, and messages.

FTP server availability

Finally, if the FTP server is unavailable at the time the backup runs, the backup will fail. You should ensure that maintenance on the FTP server occur only during times when a backup now or

scheduled backup are not run. Lastly, a backup can require 30 to 40 minutes, or even more, depending on the size of your files and the network's traffic.

Restoring backed-up system files

The messaging information stored on a server during the data backups is used to restore the system to an operational state. If your ftp server has a UNIX or Linux operating system, you start with the View/Restore screen. If your ftp server has a Windows operating system, you start with the Backup Logs screen.

If a system problem or failure occurs, backups can be invaluable in returning the system to an operational state. You are likely to restore backups when directed to do so by an alarm repair action.

Backup verification

It is recommended that you verify the success of each backup you run. The **Backup Logs** screen, available from the Server (Maintenance) Web page, allows you to verify backups. And since a backup can include a variety data types, including Communication Manager server data, the Backup Logs screen allows you to open a backup file to verify what data types are included.

Note:

Unlike other versions of messaging systems (for example, INTUITY AUDIX R5.1), there is no partial success of a backup. A Communication Manager Messaging backup is successful only if it includes all data you select for backup. If any of the data fails to be backed up, no data is stored.

Backing Up System Files Now

About the Backup Now

Use Backup Now when you want to back up system data immediately. For example, you may want to back up data very soon after you have installed the Communication Manager server and/or the messaging system. Additionally, you may want to run the backup procedure just before making a change to your system. Doing so ensures that the most recent data is backed up, including data that is new since the last scheduled backup was run.

Note:

The "backup now" does not cause a degradation in service. However, for best results, perform a backup now at a time when the messaging system experiences low usage.

Additionally, the messaging backup files can be quite large. As a result, your LAN network connection may fail during the backup. In this case, you can run a scheduled backup instead, which allows the Communication Manager server to handle breaks in the LAN connection and ultimately create a successful backup. To run a scheduled backup in case of a failed backup now, you can simply set the schedule to run on the current day and 5 or 10 minutes in the future. See Create (add) a new backup schedule on page 307.

Note:

Unlike other versions of messaging systems (for example, INTUITY AUDIX R5.1), there is no partial success of a backup. A Communication Manager Messaging backup is successful only if

it includes all data you selectfor backup. If any of the data fails to be backed up, no data is stored.

Performing a Backup Now

About this task

Note:

It is highly recommended that you stop the messaging software (voice system) before performing an attended backup. See Stopping the Messaging Software (Voice System) on page 108 for more information.

To perform a backup now:

Procedure

1. Stop the messaging software (voice system).
2. Login to the **Server (Maintenance)** Web page main menu.
3. Select:

   Backup Now

   The system displays the **Backup Now screen**.
4. Click the **Messaging** check box.
5. Click the button for the data type or data types you want to back up from the following options:

   - Messaging Announcements
   - Messaging Translations and Messages
   - Messaging Translations, Names and Messages
   - Messaging Translations and Names
   - Messaging Translations

   Only one option in the list can be selected for a specific back up. For detailed information about data sets and backup methods, see Overview of Backup and Restore on page 300.
6. Select the backup method FTP, SFTP or SCP. If you select FTP, you must start the FTP server before backing up.
7. Complete the following fields:

   User name You must enter a valid user name to enable the Communication Manager server to log in to the FTP, SFTP or SCP server. If you want to use the anonymous account, type "anonymous" in this field. If you do not want to use the anonymous account, type the actual user name in this field. Contact the FTP, SFTP or SCP server administrator if you have questions.

Password You must enter a password that is valid for the user name you entered. If you are using anonymous as the user name, you must use your email address as the password. However, the FTP site may have a different convention. Contact the FTP server administrator if you have questions.

Host name Enter the DNS name or IP address of the FTP server to which the backup data is sent. To enter an IP address, use the dotted decimal notation (for example, 192.11.13.6).

Directory Enter the directory on the corporate repository to which you want to copy the backup file. When you enter a forward slash (/) in the directory field, the system copies the backup file to the default directory. The default directory for backup data on the FTP server is /var/home/ftp. If you do not want to use the default directory, you must enter the path name for the directory. Contact the FTP server administrator if you have questions. For SCP, enter the path for the backup image file on the SCP server. This backup image is displayed for previewing or restoring.

8. If you want to encrypt the backup data, click the box in the Encryption area of the screen and enter a pass phrase using an arbitrary string of 15 to 256 characters.

   The pass phrase can contain any characters except the following ones:

   ```
   ' \ & ` " %
   ```

   It is strongly recommended that you encrypt the backup data. You must remember the pass phrase because you cannot restore the data without it.

9. Click **Start Backup**.

   The system displays the results of your backup procedure on the Backup Now results screen. If the results are not shown soon, you can also check the backup status on page 303.

10. Start the voice system.

Checking the backup status

Procedure

1. Select the **Backup History** option from the Server (Maintenance) Web page main menu.

   The system displays the **Backup History screen**.

2. Click the most recent backup in the list, and click **Check Status**.

   The system displays the **Backup History Results screen**.

3. Repeat steps 1 and 2 until the message BACKUP SUCCESSFUL appears.

Messaging data will have one of the following names attached to the backup file name:

- audix-ann for announcements
- audix-tr-msg for translations and messages
- audix-tr-name-msg for translations, names, and messages
- audix-tr-name for translations and names
- audix-tr for translations only

Note:

If your backup fails, it may be because of LAN network problems and the size of the backup file. In this case, you can run a scheduled backup instead, which allows the Communication Manager server to handle breaks in the LAN connection and ultimately create a successful backup. To run a scheduled backup in case of a failed backup, you can simply set the schedule to run for the current day of the week at a time 5 or 10 minutes in the future. See Create (add) a new backup schedule on page 307.

Backing Up System Files (Scheduled)

About the Schedule Backup

The schedule backup runs automatically, based on the schedule you create. The scheduled backup can contain all of the information necessary to bring the messaging system back to an operational state after a service-affecting event. However, the scheduled backup alone might not completely restore the system to its previous state. Depending on the severity of the situation, the messaging software might have to be reinstalled before you can restore any backups.

When scheduling the backups, follow the normal rules that apply to backup procedures. That is, be sure to schedule the backups to run outside of peak times when call processing on the server is at a minimum.

Scheduled backups do not require supervision. However, for the backup to be successful, you must ensure that the destination server to which messaging sends backup data still has space to accept a new backup

Avaya recommends that the system administrator check the Backup log daily to ensure that a successful scheduled backup occurred. If a successful scheduled backup did not occur, the system generates the MT BACKUP 1 warning alarm.

Note:

Unlike other versions of messaging systems (for example, INTUITY AUDIX R5.1), there is no partial success of a backup. A Communication Manager Messaging backup is successful only if it includes all data you selectfor backup. If any of the data fails to be backed up, no data is stored.

Creating a new backup schedule

Before you begin

Do the following:

1. Decide what type of data you want to back up.
2. Indicate the days and time you want the schedule to run.
3. Indicate the destination to which you want the backup files sent.

Procedure

1. Open a Web browser and in the **Address** field, type the IP address or FQDN of the Communication Manager Messaging System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. Click **Schedule Backup**.

   If backups are already scheduled, the screen lists the current backup schedules. Look at it carefully to determine what backup schedule you want to add.

   If this is the first backup schedule to be created, the Schedule Backup screen displays a message that there is no record of any backup schedule.

   The system displays the Schedule Backup screen.
4. Click the **Add** button at the bottom of the screen.

   The system displays the Add New Schedule screen.
5. Select the **Messaging** check box at the top of the messaging list of options.
6. Click the button for the data types that you want to back up.

   Only one option in the list can be selected for a specific back up. For detailed information about data sets, see Overview of Backup and Restore on page 300.
7. Select a backup method to indicate the destination to which the system sends the backup data.

   For detailed information about backup methods, see Overview of Backup and Restore on page 300.
8. If you want to encrypt the backup data, do the following:
   a. Click the box in the Encryption area of the screen.
   b. Enter a pass phrase using an arbitrary string of 15 to 256 characters.

   It is strongly recommended that you encrypt the backup data. You must remember the pass phrase because you cannot restore the data without it.
9. **(Optional)** If necessary, scroll to the bottom of the screen.

Select the days of the week by clicking the appropriate check boxes, and select the hour and minute you want the backup procedure to start by selecting a time from the drop-down boxes.

You can select multiple days but only one time for the backup schedule to run.

10. Click the **Add New Schedule** button to save the schedule you just created.

    The system displays the Schedule Backup screen, which adds the new backup schedule to the bottom of the schedule list.

Change a backup schedule

About this task

You can change the days and time an existing backup schedule runs. You can also change the destination to which the system sends the backup data.

To change an existing backup schedule:

Procedure

1. Log on to Communication Manager Messaging System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. On the Server Administration interface, select **Data Backup/Restore** > **Schedule Backup**.

   The system displays the Schedule Backup screen.
4. Click the radio button next to the backup schedule you want to change.
5. Click the **Change** button at the bottom of the screen.

   The Change Current Schedule screen displays the information for the backup schedule you selected in step 2.
6. Make changes to the backup schedule.

   Note:

   For detailed information about data sets, backup method, encryption, and timing for the backup schedule, see Overview of Backup and Restore on page 300.
7. Click the **Change Schedule** button to save the schedule you just created.

   The system displays the Schedule Backup screen, which lists the changed backup schedule.

Delete a backup schedule

Procedure

1. Log on to Communication Manager Messaging System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.

3. Select **Schedule Backup**.

   The system displays the Schedule Backup screen.

4. Click the radio button next to the backup schedule that you want to delete.
5. Click the **Remove** button at the bottom of the screen.

   The system removes the backup schedule that you deleted from the list displayed in the Schedule Backup screen.

Verifying a backup using the backup log

About this task

Note:

Using the backup log is the recommended method of verifying the success or failure of the of the backup.

Procedure

1. Log on to Communication Manager Messaging System Management Interface.
2. Click **Administration** > **Server (Maintenance)**.
3. On the Server Administration interface, select **Data Backup/Restore** > **Backup Logs**.

   The system displays the Backup Logs screen.

4. Look through the log until you see a backup image you want to preview or restore, and click the radio button to the left of the image.

   If no entries exist in the backup log, you will see a message that there is no record of any backups.

   Each image contains the following information:

   - Data set. Indicates which data set was backed up. If you selected more than one data set at the time of the backup, each data set is listed separately. Possible messaging data sets are:
     - Messaging translations
     - Names
     - Messages and greetings
     - Announcements

     Other data sets of the Communication Manager server may also be included, depending on how the backup was administered.
   - File size. Shows the size of the backup file.
   - Date. Shows the year, month, and day the backup was run.
   - Time. Shows the hour, minute, and second the backup was run.

- Status. Shows whether or not the backup was successful.
- Destination. Indicates how the data was recorded. It corresponds to the backup method used for the backup. Possible destinations are:
  - FTP
  - SFTP
  - SCP

5. Click **View**.

   The system displays the View/Restore Data Results screen.

6. In the **Username** and **Password** fields, type the username and password used to access the FTP, SFTP, or SCP server while backing up data.
7. Click **Preview**.

   The system updates the View/Restore Data Results screen with the data available in the image file.

Restoring Backed-Up System Files

About Restoring Backed-Up System Files

If a system problem or failure occurs, backups can be invaluable in returning the system to an operational state. You are likely to restore backups when directed to do so by an alarm repair action. Depending on the severity of the situation, messaging software might have to be reinstalled before you can restore any backups.

The messaging information stored on an SFTP/FTP/SCP server during the data backups is used to restore the system to an operational state.

Note:

Only perform a restore if a system problem or failure occurs. If you are not sure if it is necessary to perform a restore, contact your remote support center.

Performing a Restore (UNIX/Linux-based FTP Server)

About this task

Note:

Contact your remote support center if you need help restoring your system.

Note:

You must stop your messaging system before you restore data. See the instructions that follow.

The time required for a restore depends on the amount of data on the system and the speed of LAN traffic. The following procedure works for both attended and unattended backups.

Procedure

1. Stop the messaging software (voice system).
2. On the **Server (Maintenance)** web page, select **View/Restore Data**.

   The system displays the View/Restore screen.

   Note:

   If you have a Window-based FTP server, see Performing a Restore (Windows-based FTP Server) on page 312.
3. On the View/Restore Data screen, select one of the following options by clicking the corresponding radio button:
   - SFTP/ FTP/ SCP. Before the SFTP, FTP or SCP server transfers the backup image, the Communication Manager server must first log in to the server. You must therefore also enter the following information:
     - User name. Enter "anonymous" if you are using an anonymous account. Otherwise, enter your real user name.
     - Password. If you are using an anonymous account, you will typically enter your email address as the password. However, you should check with the FTP server administrator to verify this. If you are not using an anonymous account, enter your real password.
     - Host name. Enter the DNS name or IP address of the FTP server on which the data was backed up. Use the dotted decimal notation to enter IP addresses (for example, 192.11.13.6).
     - Directory. Enter the path name for the directory in which the data is stored on the remote server. Contact the remote server administrator if you have questions.
   - Local directory. Choose this selection if you know the backup image was saved to a local directory. You must enter the path name for the directory. The default directory is /var/home/ftp.
4. Click View.

   The **View/Restore Data results** screen lists the backup images stored in the location you specified. The most recent backups are listed at the bottom of the list.

   You must select a backup image before you click View, or an error message appears. To clear it, simply click the browser's Back button, then select a backup image.
5. Select the backup image you want to view or restore by clicking the corresponding radio button.

   If you must restore the Communication Manager server data sets as well as the messaging data sets, you restore the Communication Manager server data first. If the hard drive is new, and the release number of the software on the hard drive is more recent than that of the backup data, click on **Force restore if backup version mismatch** and Force Restore if server name mismatch.

6. Click one of the following buttons:
   - Preview. Use the Preview button if you are not sure you have selected the correct backup image. When you click Preview:
     - A **View/Restore Data Results** screen displays a brief description of the data associated with the backup image.
     - Messaging data will have one of the following names attached to the backup file name:
       - audix-ann for announcements
       - audix-tr-msg for translations and messages
       - audix-tr-name-msg for translations, names, and messages
       - audix-tr-name for translations and names
       - audix-tr for translations only
     - You can then click **Restore** on this second screen to begin the restore process. If the hard drive is new, and the release number of the software on the hard drive is more recent than that of the backup data, click on **Force restore if backup version mismatch** and **Force Restore** if server name mismatch.
   - Restore. When you click Restore, the system displays a View/Restore Data results screen that tells you whether or not the restore procedure is successful.
7. Do one of the following:
   - If you do not have any remote networked machines, continue with step 8 on page 310.
   - If you have any remote networked machines, do the following:
     a. Go to the **Communication Manager Messaging** > **Server Administration Request Remote Update** web page.
     b. Run a manual update to and from all remote networked machines to correct any database inconsistencies.

        See Running a Remote Update Manually on page 140.
     c. Continue with step 8 on page 310.
8. Restart the Communication Manager software.

Performing a Restore (Windows-based FTP Server)

Procedure

1. Stop the messaging software (voice system).
2. On the Server (Maintenance) page, select **Backup Logs**.

   The system displays the Backup Logs screen.
3. Select the backup image you want to preview or restore by clicking the corresponding radio button.

If you must restore the Communication Manager server data sets as well as the messaging data sets, you restore the Communication Manager server data first. If the hard drive is new, and the release number of the software on the hard drive is more recent than that of the backup data, click on **Force restore if backup version mismatch** and **Force Restore** if server name mismatch.

4. Click one of the following buttons:

   - Preview. Use the Preview button if you are not sure you have selected the correct backup image.

   The system displays the Preview Data screen.

   On the Preview Data screen, enter the following data:

   - User name. Enter "anonymous" if you are using an anonymous account. Otherwise, enter your real user name.
   - Password. If you are using an anonymous account, you will typically enter your email address as the password. However, you should check with the remote backup server administrator to verify this. If you are not using an anonymous account, enter your real password.
   - Pass phrase. Enter the encryption password, if any. If there is no encryption password, leave the field blank.

   Click the **Preview** button.

   - The View/Restore Data Results screen displays a brief description of the data associated with the backup image.
   - Messaging data will have one of the following names attached to the backup file name:
     - audix-ann for announcements
     - audix-tr-msg for translations and messages
     - audix-tr-name-msg for translations, names, and messages
     - audix-tr-name for translations and names
     - audix-tr for translations only
   - You can then click **Restore** on this second screen to begin the restore process. If the hard drive is new, and the release number of the software on the hard drive is more recent than that of the backup data, click on **Force restore if backup version mismatch** and **Force Restore** for server name mismatch.
   - When you click **Restore**, the system displays the Restore Data screen.

   On the Restore Data screen, enter the following data:

   - User name: Enter "anonymous" if you are using an anonymous account. Otherwise, enter your real user name.
   - Password: If you are using an anonymous account, you will typically enter your email address as the password. However, you should check with the FTP server administrator to verify this. If you are not using an anonymous account, enter your real password.

- Pass phrase: Enter the encryption password, if any. If there is no encryption password, leave the field blank.
- If the hard drive is new, and the release number of the software on the hard drive is more recent than that of the backup data, click on **Force restore if backup version mismatch** and **Force Restore** if server name mismatch.

Click the **Restore** button. When you click **Restore**, the system displays a View/Restore Data results screen that tells you whether or not the restore procedure is successful.

If the results are not shown soon, you can also check the status using the following steps:

a. Select the **Restore Status** option from the main menu.

   The system displays the **Restore Status Selection** screen.

b. Click the most recent restore in the list, and click Check Status.

   The system displays the Restore Status screen.

   Note:

   The **Refresh** button is not available for this release of software.

c. Repeat steps a and b until the system displays the `Restore of backup image completed successfully` message.

5. Do one of the following:
   - If you do nothave any remote networked machines, continue with step 6.
   - If you have any remote networked machines, do the following:
     a. Logoff from the Communication Manager server.
     b. Log in to the Communication Manager Messaging web page.
     c. Run a manual update to and from all remote networked machines to correct any database inconsistencies.

        See Running a Remote Update Manually on page 140.
6. Restart Communication Manager software.

Appendix A: Microsoft Outlook configuration

For information about setting up Microsoft Outlook 2010, see the *Technical White Paper for Internet Messaging Feature on Avaya Communication Manager Messaging server (CMM)* at https://downloads.avaya.com/css/P8/documents/101014853.

Appendix B: Centralized Messaging Server configuration

Use the procedures in this section as a guideline to configure the remote and host server or Centralized Messaging Server.

Configuring the Remote Server with translation data

Establish coverage path for Communication Manager Messaging

Procedure

1. Log in to Communication Manager and access the SAT command line interface.
2. Type `add coverage path n`, where *n* is the coverage path number.

   For example, type `add coverage path 60`.
3. In the **Point 1** field, type the number for coverage point 1.
4. Save the changes.
5. Type `add station nnnnn`, where *nnnnn* is the extension number.

   For example, type `add station 60000`.
6. Type appropriate values in the **Type**, **Security Code**, **Name**, and **Coverage Path 1** fields.
7. Go to page 2.
8. In the **MWI Served User Type** field, type `qsig-mwi`.
9. Save the changes.
10. Type `add hunt-group n`, where *n* is the hunt group number.

    For example, type `add hunt-group 60`.
11. Type appropriate values in the **Group Name** and **Group Extension** fields.

12. Go to page 2.
13. In the **Message Center** field, type `qsig-mwi`.
14. In the **Voice Mail Number** field, type a voice mail number.
15. Save the changes.

Setup routing to Centralized Messaging Server

Procedure

1. Log in to Communication Manager and access the SAT command line interface.
2. Type **change dialplan analysis**.
3. Type appropriate values in the **Dialed String**, **Total Length**, and **Call Type** fields.
4. Save the changes.
5. Type `change uniform-dialplan n`.

   The system lists entries that begin with or are greater than the number n. For example, if you type change uniform-dialplan 7, the system lists entries beginning with 7. If no matching patterns begin with 7, the system lists entries beginning with a number greater than 7.
6. Type appropriate values in the **Matching Pattern**, **Len**, **Del**, and **Net** fields.
7. Save the changes.
8. Type `change aar analysis n`, where *n* is the digit string.
9. Type appropriate values in the **Dialed String**, **Total Min**, **Total Max**, **Route Pattern**, and **Call Type** fields.
10. Save the changes.
11. Type `change route-pattern n`, where *n* is the route pattern number.
12. Type appropriate values in the **Pattern Name**, **Grp No**, **FRL**, **TSC**, and **CA-TSC Request** fields.

    The pattern name is the name of the remote server.
13. Save the changes.

Create tie trunk to the Centralized Messaging Server

Procedure

1. Log in to Communication Manager and access the SAT command line interface.
2. Type `add trunk-group n`, where *n* is the trunk group number.
3. In the **Group Type** field, type `isdn`.

4. In the **Group Name** field, type the name of the trunk group.

   For example, in the **Group Name** field, type `tie to remote server 1`.
5. In the **TAC** field, type the trunk access code that must be dialed to access the trunk group.
6. In the **Carrier Medium** field, type the transport medium interface used for the ISDN trunk group.
7. In the **Dial Access?** field, specify whether users can route outgoing calls through an outgoing trunk group.
8. In the **Service Type** field, type `tie`.
9. In the **Member Assignment Method** field, type the method used to assign trunk members to a signaling group.
10. In the **Signaling Group** field, type the assigned signaling group number.

    Since the signaling group is not defined at this stage of configuration, you must revisit this SAT screen and assign the signaling group after creating the signaling group
11. In the **Number of Members** field, type the number of virtual trunk members automatically assigned to the signaling group.
12. Go to page 2.
13. Type appropriate values for the **Supplementary Service Protocol** and **Format** fields.
14. Go to page 3.
15. Type appropriate values for the **NCA-TSC Trunk Member**, **Send Name**, and **Send Calling Number** fields.
16. Save the changes.
17. Type `change node-names ip`.
18. In the **Name** field, type the name of the remote server.
19. In the **IP Address** field, type the IP address of the remote server.
20. Save the changes.
21. Type `add signaling-group n`, where *n* is the signaling group number.
22. In the **Group Type** field, type `sip`.
23. In the **Transport Method** field, type `TLS` or `TCP`.
24. In the **Near-end Node Name** field, type the node name for the C-LAN IP interface in the Avaya S8XXX server.
25. In the **Far-end Node Name** field, type the node name for the far-end IP interface that is used for trunks assigned to the signaling group.
26. In the **Far-end Listen Port** field, type the port number administered for the near-end listen port.

27. In the **Far-end Network Region** field, type the number of the network region that is assigned to the far-end of the signaling group.
28. Save the changes.

Setup calling party number for call answer, otherwise hear ext 00000

Procedure

1. Log in to Communication Manager and access the SAT command line interface.
2. Type `change private-numbering n`, where *n* is the length of the extension.
3. In the **Ext Len** field, type the number of digits that the extension can have.
4. In the **Ext Code** field, type the code for the extension.
5. In the **Total Len** field, type the total number of digits to send.
6. Save the changes.

Setup calling party number for login to messaging with # (extension not entered)

Procedure

1. Log in to Communication Manager and access the SAT command line interface.
2. Type `change public-unknown-numbering n`, where *n* is the extension length.
3. In the **Ext Len** field, type the number of digits that the extension can have.
4. In the **Ext Code** field, type extension code.
5. In the **Total CPN Len** field, type the number of digits that the extension can have.
6. Save the changes.

Setup routing of Message Waiting Indicator back to the remote server

Configuring the host server

Procedure

1. Log in to Communication Manager and access the SAT command line interface.
2. Type `change uniform-dialplan n`.

   The system lists entries that begin with or are greater than the number n. For example, if you type change uniform-dialplan 4, the system lists entries beginning with 4. If no matching patterns begin with 4, the system lists entries beginning with a number greater than 4.
3. Type appropriate values in the **Matching Pattern**, **Len**, **Del**, and **Net** fields.
4. Save the changes.
5. Type `change aar analysis n`, where *n* is the digit string.
6. Type appropriate values in the **Dialed String**, **Total Min**, **Total Max**, **Route Pattern**, and **Call Type** fields.
7. Save the changes.
8. Type `change route-pattern n`, where *n* is the route pattern number.
9. Type appropriate values in the **Pattern Name**, **Grp No**, **FRL**, **TSC**, and **CA-TSC Request** fields.

   The pattern name is the name of the remote server.
10. Save the changes.

Creating tie trunk to remote server

About this task

Ensure that the trunk group number, and the signaling group number is the same number used when creating tie trunk to the host server.

Procedure

1. Log in to Communication Manager and access the SAT command line interface.
2. Type `add trunk-group n`, where *n* is the trunk group number.
3. In the **Group Type** field, type `isdn`.
4. In the **Group Name** field, type the name of the trunk group.

For example, in the **Group Name** field, type `tie to remote server 1`.

5. In the **TAC** field, type the trunk access code that must be dialed to access the trunk group.
6. In the **Carrier Medium** field, type `h.323`.
7. In the **Dial Access?** field, type `y`.
8. In the **Service Type** field, type `tie`.
9. In the **Member Assignment Method** field, type `auto`.
10. In the **Signaling Group** field, type the assigned signaling group number.

    Since the signaling group is not defined at this stage of configuration, you must revisit this SAT screen and assign the signaling group after creating the signaling group
11. In the **Number of Members** field, type the number of virtual trunk members automatically assigned to the signaling group.
12. Go to page 2.
13. In the **Supplementary Service Protocol** field, type `b`.
14. In the **Format** field, type `unk-pvt`.
15. Go to page 3.
16. In the **NCA-TSC Trunk Member** field, type `1`.
17. In the **Send Name** field, type `y`.
18. In the **Send Calling Number** field, type `y`.
19. Save the changes.
20. Type `change node-names ip`.
21. In the **Name** field, type the name of the remote server.
22. In the **IP Address** field, type the IP address of the remote server.
23. Save the changes.
24. Type `add signaling-group n`, where *n* is the signaling group number.
25. In the **Group Type** field, type `sip`.
26. In the **Transport Method** field, type `TLS` or `TCP`.
27. In the **Near-end Node Name** field, type the node name for the C-LAN IP interface in the Avaya S8XXX server.
28. In the **Far-end Node Name** field, type the node name for the far-end IP interface that is used for trunks assigned to the signaling group.
29. In the **Far-end Listen Port** field, type the port number administered for the near-end listen port.

30. In the **Far-end Network Region** field, type the number of the network region that is assigned to the far-end of the signaling group.
31. Save the changes.

Appendix C: (Deprecated) Message Manager

Note:

Message Manager is now deprecated.

Capabilities and Benefits

(Deprecated) Message Manager offers product capabilities that facilitate the way subscribers organize their messages.

Capabilities

(Deprecated) Message Manager includes the following basic capabilities:

- Visual display of the messaging mailbox, with the ability to play or view any component, including voice through a simple GUI
- A Personal Phonebook for storing addresses and important information on a PC, independent of the messaging software
- Support for playing and recording messages, greetings, and names on a PC sound card
- Remote access to your messages through a high-speed modem
- The ability to receive, create, and send voice messages, text messages, and attached files
- The ability to send and receive email messages through Message Manager with Internet Messaging
- Ability to receive, forward, delete, print, or create fax messages
- Message annotation
- Nonsequential message retrieval
- Advanced playback controls
- Archival of Communication Manager Messaging messages to the PC hard drive
- Outcalling notification
- Support for multiple greetings

Requirements to Run (Deprecated) Message Manager

(Deprecated) Message Manager requires client software and minimum hardware standards and a LAN connection to the messaging server.

Software and Hardware Requirements

For Message Manager 4.5 and later, the following minimum requirements are necessary to support Message Manager:

- Minimum of a 486, 66 MHz PC with 16 MB of RAM and 19 MB of available hard disk storage (assuming a Personal Address Book with 400 entries).

  Exceptions include:

  - The tutorial requires an additional 10 MB of disk storage.
  - Possible additional RAM is needed by your operating system for better performance (for example, 32 MB of RAM for Windows NT).
- VGA or higher monitor (color recommended)
- LAN interface card
- Windows Sockets (WINSOCK.DLL) access to TCP/IP (either through a NetWare Loadable Module or a TCP/IP protocol stack)
- Recommended: Mouse supported by Microsoft Windows
- Optional Equipment:
  - Speaker Phone
  - Telephone headset
  - A Microsoft Windows-compatible soundcard with speakers
  - A microphone, or a computer headset for hands-free operation

One of the following compatible operating systems:

- Windows 7 and higher

  Note:

  You must use the compatibility mode and ignore FAX driver errors.

LAN and the Messaging Server Requirements

Requirements for the local area network (LAN) include:

- LAN configuration that provides TCP/IP transport between the messaging server and client PC
- Ethernet network with valid physical connection: either Gigabit Ethernet, 100BaseT, 10BaseT, 10Base2 (thin coax), or 10 Base5 (thick coax) for a messaging server
- A customer-provided router or other device to convert token-ring protocol to the required Ethernet protocol if Message Manager is to communicate with a token-ring network

Internet Messaging Requirements

Message Manager uses Internet Messaging to send email over the Internet. Internet Messaging requires:

- Two dedicated trusted servers (automatically installed on a new messaging system)
- Professional Services (highly recommended) for consultation and implementation assistance.

System Capacity

The following system capacities apply:

- Up to 300 clients can be registered at one time. A client is registered when a subscriber starts the client application from a PC, which invokes a TCP/IP session. (Subscribers must exit the client application to "unregister" the client.)
- Up to 64 messaging login sessions can be in progress at any one time, depending on the messaging platform used. A messaging login session starts when a subscriber logs into a messaging mailbox from a PC. The messaging software terminates a login session if a session has been inactive for the amount of time set in the **LAN Session Timeout** field on the System-Parameters MCAPI-Options screen. However, the client registration is still active, and a messaging login session is established automatically again when the client starts using Message Manager.
- As many audio sessions as voice ports purchased can be in progress at any one time. This means that a subscriber is logged in to the messaging software (one of the up to 64 login sessions) and an audio session is active (for example, a subscriber is listening to a voice mail message). When the audio session is completed, the messaging software disconnects the voice port. The client application remains one of the messaging login sessions until the inactivity timeout takes effect or Message Manager is minimized or closed.

Messaging Enhancements

Every (Deprecated) Message Manager release offers features that add to the efficiency of any work environment. These features are summarized in the section that follows.

New Message Notification

Subscribers of (Deprecated) Message Manager receive a notification when a new message is received. This notification is either a small icon that appears in the toolbar or a pop-up window that appears on the PC screen.

From the main Message Manager screen, subscribers can view the:

- Media type component or components included in the message
- Sender of the message
- Subject of the message
- Time and date received
- Status of the message: priority, private, or partial delivery

Play or View a Message

After you select a folder, the messages stored within the folder are displayed. You can select one of the messages either to play it or to view its contents. The following explains the options available for playing or viewing a message:

- Voice
- The system plays the message through an audio connection or the sound card, depending on the selected option.
- Text
- The Text Viewer displays the message on the screen. You can read the text on the screen or print its contents to a printer.
- Attached Files
- You can view several types of files. Once you select a file from the list, you can start the corresponding program and view the file or you can export the file to your own computer.

Reply to or Forward a Message

After you play or view a message, you might want to add your comments and respond to the sender or mail it to another messaging subscriber:

Reply to Sender	You can create a message to send back to the sender by using automatic addressing. Include any or all of the original message components, plus any new components.
Forward	You can add your comments to the message you received and then send them and the original message to another messaging subscriber

Send Messages to Multiple Recipients

You can create and send a message to one or several people, with one or more message components. You can decide to deliver the message as soon as possible or schedule the message for a later delivery time.

Addressing

You can send the message to just one person or a list of people.

Use the Outgoing Folder

After a message is sent, you can check its delivery status by opening the Outgoing Folder. The Outgoing Folder lists all the messages you have sent, indicates the time when they were sent, and confirms whether the recipient has received or accessed the message. In this folder, you can access more delivery information by double-clicking a message or by highlighting a message and selecting the View Delivery Report option under the Activity pull-down menu.

Build Personal Phonebook

You can use the Personal Phonebook in Message Manager to store "cards" with the addresses of the messaging subscribers, as well as other numbers and notes. Once subscribers are added to the Phonebook, you can quickly add them to an address list. The Personal Phonebook is stored on your PC and can be used while you are working offline.

Build Messaging Lists

With messaging lists, you can store the addresses of sets of people to whom you want to send messages all at once, such as a project team or a corporate department. You can quickly address a message to an entire address list. messaging lists are stored on the messaging server and are not available offline.

Work Offline

If you work away from the office, you might want to edit messages that you have received or compose new messages and then log in later and send the messages during a single telephone call. This procedure saves toll charges because a messaging server connection is not required.

Minimize or Lock Message Manager

You can minimize (Deprecated) Message Manager and still be notified of new messages throughout the day. Later, you can restore the program to retrieve messages or to create and send new messages.

For enhanced security, Message Manager has a Lock feature. When you select the Lock icon, the application is minimized and requires your messaging password to be restored. Locking Message Manager prevents others from accessing your messaging mailbox. This capability is inactive while you work offline.

Record Your Name or Greetings

When you install (Deprecated) Message Manager, you can use your name and personal greeting that were recorded through the messaging telephone interface. You can select a menu option to record your name or to display a screen for recording and managing greetings. The messaging software uses the choices you make in Message Manager for playing names or greetings to your callers.

Outcalling

If you are away from the office, (Deprecated) Message Manager can still notify you of new messages. Use the Outcalling feature to enter a telephone or pager number that the messaging software dials to notify you of new messages.

Sound Card

(Deprecated) Message Manager uses an audio connection to your telephone to play or record voice messages or greetings. However, you can use your computer's sound card with speakers and a microphone instead, which is also the only way to play or record your voice messages while you work offline.

Planning Considerations

An account representative works with the customer to determine the optimal configuration of software and hardware to meet present needs and future plans.

Planning the integration of (Deprecated) Message Manager with the messaging software can involve the customer's PC/LAN system administrator. Another important planning consideration is understanding that customers are responsible for installing Message Manager. Customers are

responsible whether the installation is on a PC or on a server for access by subscribers over a LAN. The application can be installed from diskettes, from a CD, or from a LAN file server.

The following sections highlight some of the major considerations customers must be aware of to take full advantage of a multimedia messaging system, such as Message Manager.

Electronic Mail Integration

There is a difference between (Deprecated) Message Manager and an email system, however Message Manager can be used to send messages to subscribers on the same messaging system or to networked and administered remote messaging systems. A supported email system, however, can be used to send messages to systems external to the messaging server, for example, the Internet or other email systems. Message Manager also supports this if Internet Messaging is enabled. See Overview of Message Manager Administration on page 331 for a complete overview of the Message Manager.

In many situations, a customer site may have a voice mail system and a separate email messaging system. To retrieve all messages, subscribers must access each system individually. Messaging alleviates this problem with an optional feature known as Internet Messaging. This optional feature provides a gateway through which the messaging software can send and receive messages across an email network.

As with Message Manager, subscribers can choose messages in any order and, by selecting icons using a mouse, perform all messaging tasks everything that can be done with the telephone keypad. See Internet Messaging Concepts and Planning on page 280 for a complete overview of the Internet Messaging feature.

Message Size

A multimedia message that is created through Message Manager can have a significant impact on the space allocated for subscriber mailboxes. A mailbox can have up to 32767 seconds of recorded voice messages, which is approximately 262.1 MB. Files that are attached through Message Manager could fill up a mailbox very quickly.

LAN Impact

The messaging system is viewed as a server on a LAN. The PC/LAN system administrator at a customer's site should handle LAN installation, administration, and troubleshooting.

Use the information in the table for Impact of Message Manager on LAN Traffic on page 323 to calculate how much of the LAN traffic on a system is expected to be comprised of Message Manager messages (including messages with attached components) based on the number of messages that a typical subscriber generates during a busy hour.

Impact of Message Manager on LAN Traffic

Component Type	Packet Size Distribution	Message Manager (Packets per Hour)	Message Manager (Packets per Second)
Voice (without sound card)	• 96% small packet messages (100 bytes) • 4% large packet messages (1 KB)	102 (without sound card)	102 (packets/hour/ subscriber) timesnumber of subscribers dividedby3600 (seconds/ hour)

Table continues…

Component Type	Packet Size Distribution	Message Manager (Packets per Hour)	Message Manager (Packets per Second)
Voice (with sound card)	• 50% small packet messages (100 bytes) • 50% large packet messages (1 KB)	111 (with sound card)	111 (packets/hour/ subscriber) timesnumber of subscribers dividedby3600 (seconds/ hour)
Message Manager text message	• 33% small packet messages (100 bytes) • 67% large packet messages (1 KB)	25	25 (packets/hour/ subscriber) timesnumber of subscribers dividedby3600 (seconds/ hour)

Message Manager is a Windows-based graphical user interface (GUI) that allows Communication Manager Messaging messages to be viewed on a PC screen through a local area network (LAN) or dial-up connection. Subscribers with Message Manager can create, send, and receive messages that contain multiple media typesvoice, text, or file attachments (attached software files).

The visual aspects of Message Manager distinguishes it from other voice messaging products. Message Manager allows you to view the name of the person who sent the message, a brief subject that describes the message, the time and date that the message was received, and the type of message that was received. This information helps subscribers prioritize how they access messages and develop mailing lists more easily.

Message Manager is available in seven languagesEnglish, French, Spanish, Brazilian Portuguese, German, Dutch, and Italian. Additional languages are being considered for future releases.

Addressing a Fax Message with (Deprecated) Message Manager 4.6 or Later

When addressing a Fax message in (Deprecated) Message Manager 4.6 or later, verify that the Fax number has a prefix that is a trunk access code, usually 9, and has the suffix @Fax. For example, if the number you are Faxing is 011-4122-734-2803, then enter 901141227342803@Fax. See Examples of Fax Addressing in Message Manager on page 265 for more examples of how to address a Fax message for specific call types in Message Manager 4.6 or later.

Call Type	Fax Number	Enter
Local 7-digit number	275-5555	92755555@Fax
Local 10-digit number	303-555-1234	93035551234@Fax
US long distance number	213-555-9999	912135559999@Fax
International number (up to 23 digits)	011-4122-734-2803	901141227342803@Fax

Creating a Fax Message with (Deprecated) Message Manager 4.6 or Later

About this task

To create a Fax message in Message Manager 4.6 or later:

Procedure

1. Create a document in any software application that has print capabilities.
2. Select **File > Print**.
3. In the print dialog box, select **Message Manager Fax Print Driver**(or, **MM Fax Print Driver**).
4. Click:

   OK.
5. The (Deprecated) Message Manager program opens and creates a new message with a Fax component.
6. Add additional components if you want.
7. Address the message in the following format:

   <number>@Fax

PC Access through (Deprecated) Message Manager

(Deprecated) Message Manager is a software application that runs on a Windows-based PC and connects with Communication Manager Messaging through a TCP/IP LAN. The program uses a graphical interface to enable subscribers to view a list of their messages on their personal computers. Subscribers can choose messages in any order and, by selecting icons with a mouse, perform all messaging tasks that can be done with a telephone keypad and more.

(Deprecated) Message Manager can be used to create and send text and voice messages to subscribers on the same messaging system or to networked and administered remote messaging systems. Additionally, with Message Manager, you can attach binary files to messages or receive and open binary files.

See Overview of Message Manager Administration on page 331 for a complete overview of (Deprecated) Message Manager.

Communication Manager Messaging is a feature that integrates voice, Fax, text messages, and attachments into a single system and offers subscribers enhanced flexibility to manage messages from their telephones or personal computers.

Note:

Message Manager is deprecated. You can use the standards based email clients such as Microsoft Outlook to manage mailboxes, folders and messages. There is no separate user interface for subscriber configuration

(Deprecated) Message Manager Administration

Overview of (Deprecated) Message Manager Administration

This section explains how to administer the messaging subscribers for (Deprecated) Message Manager.

Before You Continue

Before you use this section, verify that:

- (Deprecated) Message Manager is installed and administered on your client workstation.
- All necessary LAN installation and configuration is complete.

See Also

For additional information about (Deprecated) Message Manager, see:

- Information in the (Deprecated) Message Manager concepts and features section about:
- - (Deprecated) Message Manager on page 323
  - Requirements to Run (Deprecated) Message Manager on page 324
  - Messaging Enhancements on page 325
  - (Deprecated) Message Manager on page 323
- The user's guide or administrator's guide for your release of (Deprecated) Message Manager

Enabling Subscribers for (Deprecated) Message Manager

Now that the platform is administered to handle the (Deprecated) Message Manager application, you must give subscribers access to (Deprecated) Message Manager. There are two ways in which you can enable subscribers for (Deprecated) Message Manager:

- On an individual (subscriber-by-subscriber) basis
- By defining a Class of Service (COS)

If you have a large number of subscribers to administer, defining or revising a COS is more efficient than enabling each subscriber individually.

Note:

The following tasks contain instructions that relate only to the one or two fields on a particular screen that are part of (Deprecated) Message Manager administration. See Subscriber Administration on page 91 for complete field descriptions.

Enabling (Deprecated) Message Manager on an Individual Basis

About this task

To administer an individual subscriber for (Deprecated) Message Manager:

Procedure

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

   System displays the Manage Subscribers page.
4. Click **Manage** for the **Local Subscribers**.

   The system displays the Manage Local Subscribers page.
5. Select the subscriber from the list and click the **Edit/Delete the Selected Subscriber**.

   The system displays the Edit Local Subscriber page.
6. In the **PERMISSIONS** group, perform the following actions:
   a. In the **MCAPI Access** field, select **yes**.
   b. In the **MCAPI Message Transfer** field, select **yes**.

   Security alert:

   Allowing MCAPI and trusted server access increases the possibility for toll fraud. For more information see System Security on page 251.
7. In the **MISCELLANEOUS** group, perform the following actions:
   a. In the **Voice Mail Message (seconds), Maximum Length** field, type `1200`.
   b. In the **Call Answer Message (seconds), Maximum Length** field, type `1200`.
   c. In the **Mailbox Size (seconds), Maximum** field, type `12000`.
8. Click **Save**.

Enabling (Deprecated) Message Manager by Defining a COS

About this task

To administer predefined groups of subscribers for (Deprecated) Message Manager:

Procedure

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

   The system displays the Manage Classes-of-Service page.
4. Select the class-of-service that you want to edit and click **Edit the Selected COS**.

   The system displays the Edit a Class-of-Service page.
5. In the **PERMISSIONS** group, perform the following actions:
   a. In the **MCAPI Access** field, select **yes**.
   b. In the **MCAPI Message Transfer** field, select **yes**.

   Security alert:

   Allowing MCAPI and trusted server access increases the possibility for toll fraud. For more information see System Security on page 251.
6. In the **MISCELLANEOUS** group, perform the following actions:
   a. In the **Voice Mail Message (seconds), Maximum Length** field, type `1200`.
   b. In the **Call Answer Message (seconds), Maximum Length** field, type `1200`.
   c. In the **Mailbox Size (seconds), Maximum** field, type `12000`.
7. Click **Save**.

Troubleshooting (Deprecated) Message Manager

This section suggests remedies for some commonly encountered problems. Additional troubleshooting advice is included in the (Deprecated) Message Manager online Help and the (Deprecated) Message Manager Administration manual.

Note:

After installation, unless otherwise specified by contract, the customer is responsible for maintaining the TCP/IP addresses and for administration on the messaging system. Avaya

service technicians dispatched for messaging system installation and maintenance are not allowed to troubleshoot the customer LAN unless specified by contract.

Index

Numerics

5000 274

A

activating
    announcement set 165
activity log 203
activity log data collection options
    changing 204
adding
    new enhanced list 116
    remote digital networking machine 126
    remote user 143
Add Local Subscriber
    field descriptions 95
add networked server
    field description 126
add remote subscriber
    field description 144
address ranges
    listing 133
administering
    call answer disclaimer 118
    ELA list 116
Administer System Attributes and Features
    field descriptions 58
administration history log
    field descriptions 210
administration history log report
    results page 211
administration password
    changing 37
administrator log
    field descriptions 202
    viewing 119
administrator log results
    field descriptions 203
administrators log 202
administrator's history log
    viewing 210
alarm log
    field descriptions 207
Alarm Log report results
    field descriptions 208
alarm report
    displaying 207
Alarm Summary
    field descriptions 86
announcement set
    activating 165
auto attendant
    routing holiday schedules 193
Avaya courses 10

B

beginning
    collection of traffic data 213
broadcast message
    sending 76

C

calling party number 319
call management system
    reports 250
Centralized Messaging Server
    configuration 316
changing
    administration password 37
    extension length 55
    local machine information 122
    non-administered remote subscriber options 142
    public unknown numbering 319
    Subscriber Name Recordings 103
changing block of extensions 56
changing COS
    considerations 92
checklist
    fax messaging 266
Class of service
    editing 92
Class-of-Service
    settings 113
Communication Manager Messaging network
    configuringz 31
Communication Manager server view current alarms page 209
community daily traffic
    field descriptions 216
    viewing 215
community hourly traffic
    report 217
    viewing 217
Community Hourly Traffic report
    field descriptions 218
configure subscriber activity log
    field descriptions 204
configuring
    Communication Manager Messaging network 31
creating
    Subscriber Name Recordings 103
    tie trunk to remote server 320
current alarms

current alarms *(continued)*
viewing 209
customizing
announcements 147

D

deleting
remote machines 132
remote user manually 145
digital networking
initial administration 120
displaying
alarm report 207

E

editing
networked servers 139
edit messaging server
field descriptions 123
ELA list
administering 116
email access
telephone 281
enabling
automatic mail forwarding to SMTP 104
IPv6 33
enhanced list
adding 116
events log
viewing 211
example
GOS 246
Grade of Service 246
extension length
changing 55

F

fax messaging
checklist 266
feature daily traffic
field descriptions 219
feature daily traffic report
viewing 218
feature hourly traffic
field descriptions 222
feature hourly traffic report
viewing 221
field description
add networked server 126
report of server extension ranges 134
field descriptions
Add Local Subscriber 95
Administer System Attributes and Features 58
administration history log 210
administrator log 202
administrator log results 203
alarm log 207
Alarm Log report results 208
Alarm Summary 86
community daily traffic 216
Community Hourly Traffic report 218
edit messaging server 123
feature daily traffic 219
feature hourly traffic 222
load hourly traffic 225
load hourly traffic report 226
maintenance log 211
manage remote subscribers 134
Network Configuration 32
network load daily traffic 227
network load hourly traffic report 229
Remote Messages Daily Traffic 230
Remote Messages Monthly Traffic report 232
Special Features Daily Traffic 235
Special Features Hourly Traffic 236
Subscriber Activity Log 206
Subscriber Daily Traffic report 237
Traffic Snapshot Daily report 242
Traffic Snapshot Monthly report 244
Voice Channel Monitor Display 87

G

GOS
example 246
Grade of Service
example 246

I

interpreting
traffic reports 245
IPv6
enabling 33

L

ldap status
verifying 288
legal notice .....
listing
address ranges 133
load daily traffic report
viewing 224
load hourly traffic
field descriptions 225
load hourly traffic report
field descriptions 226
local machine information

local machine information *(continued)*
changing 122
logging in
messaging system 35

M

maintenance log
field descriptions 211
manage remote subscribers
field descriptions 134
manual administration
remote user 143
manually changing
remote user data 145
messaging software
list 85
messaging system
logging insu 35
microsoft outlook
configuration 315

N

network
configuration 31
Network Configuration
field descriptions 32
networking 25
network load daily traffic
field descriptions 227
network load daily traffic report
viewing 227
network load hourly traffic report
field descriptions 229
viewing 228
non-administered remote subscriber options
field descriptions 142

P

password
administration 36
password aging
setting 38
private numbering
changing 319
purpose 8

R

receiving
voice messages from remote test subscribers 136
recording
user name 146
related documentation 8
remote machine
renaming 130
remote machines
deleting 132
Remote Messages Daily Traffic
field descriptions 230
remote messages daily traffic report
viewing 229
Remote Messages Monthly Traffic report
field descriptions 232
viewing 232
remote subscribers
viewing 141
remote updates
overview 138
remote user
adding 143
administration 137
remote users
types 137
renaming
remote machine 130
report of server extension ranges
field description 134
reports
call management system 250
data retention 214
introduction 201
resetting
subscriber passwords 104
restarting
messaging 107
results of system status 83
running
activity log report 206

S

sending
broadcast messasge 76
voice message 135
setting
password aging 38
Special Features Daily Traffic
field descriptions 235
Special Features Daily Traffic report
viewing 234
Special Features Hourly Traffic
field descriptions 236
Special Features Hourly Traffic report
viewing 235
Subscriber Activity Log
field descriptions 206
Subscriber Daily Traffic report
field descriptions 237
Subscriber Monthly Traffic report
viewing 241

Subscriber Name Recordings
changing 103
creating 103
support 11
system problems
spotting 249
system status
verifying 82

T

TCP/IP LAN connectivity
administration 122
testing
digital networking and tcp/ip connection 135
traffic reports
interpreting 245
overview 212
Traffic Snapshot Daily report
field descriptions 242
viewing 241
Traffic Snapshot Monthly report
field descriptions 244
viewing 243
training 10

V

verifying
ldap status 288
system status 82
user name 147
videos 11
viewing
administrator log 119
administrator's history log 210
community daily traffic 215
community hourly traffic 217
current alarms 209
delivery failure log 119
events log 211
feature daily traffic report 218
feature hourly traffic report 221
hourly traffic report 225
list of machines 135
load daily traffic report 224
network load daily traffic report 227
network load hourly traffic report 228
remote messages daily traffic report 229
Remote Messages Monthly Traffic report 232
remote subscribers 141
Special Features Daily Traffic report 234
Special Features Hourly Traffic report 235
Subscriber Monthly Traffic report 241
Traffic Snapshot Daily report 241
Traffic Snapshot Monthly report 243
Voice Channel Monitor Display
field descriptions 87
voiced name 147
voice message
sending 135
voice messaging 24
voice messaging database audit 198
voice system
start messaging software 107

W

Warranty 12