Administering Avaya Aura® Messaging

Release 6.2
Issue 2.2
December 2013

Contents

Chapter 1: Introduction 15
- Purpose 15
- Intended audience 15
- Document changes since last issue 15
- Related resources 15
  - Documentation 15
  - Training 16
  - Avaya Mentor videos 17
- Support 17
- Warranty 18

Chapter 2: Preparing for Avaya Aura® Messaging 19
- Prepare your network 19
  - Network overview 19
  - DNS record 19
- Prepare for Exchange forms 20
  - Exchange administration overview 20
  - Organizational Forms Library 21
  - Installing the voice message form 24

Chapter 3: Getting started with Avaya Aura® Messaging 27
- Administration overview 27
  - System Management Interface 27
  - Administration passwords 28
  - Checklist for administrators 32
- Logging in to Messaging 33
- Logging out 35

Chapter 4: Initial administration of the storage role 37
- Initial administration checklist for the storage role 37
- Verifying the system clock 38
- Changing the LDAP root password 39
- Verifying the status of the storage role 40
- Enable outbound SMTP based traffic 41
  - Administering the external SMTP host 41
  - Add a New External Host field descriptions 42
  - Adding a mailbox gateway 42
- Setting the length of mailbox numbers 43
- Adding the postmaster mailbox 43
- Configuring the postmaster mailbox number 45
- Flexible storage 45
  - Configure the minimum required service account permissions 46
  - Configure Exchange Web Services 52
  - Configuring a storage destination 52
  - Storage Destinations field descriptions 53
  - Selecting a storage destination 55

Chapter 5: Initial administration of the application role 57

Deployment scenarios ... 57
Initial administration checklist for application roles ... 58
Telephony integration ... 59
Integration requirements ... 59
Support for SIP INFO messages on SIP connections ... 60
Integrating with the telephony server ... 60
Telephony Integration field descriptions ... 61
Telephony Integration Checklist ... 65
Implementing fax ... 66
Enabling fax ... 66
Language packs ... 67
Configuring languages ... 68
Languages field descriptions ... 69
Changing the AxC IP address ... 70
Backing up application files ... 72
Restoring application files ... 73
Messaging configuration checklist ... 74
Chapter 6: Sites and topology ... 81
Initial administration checklist for sites and topology ... 81
Initial site administration ... 82
Overview for administering sites ... 82
Improved multisite support including full E.164 Dial Plan support ... 82
Setting site properties for the first time ... 83
Dial rules ... 84
Assigning an attendant number ... 86
Adding sites on application servers ... 87
Assigning language menu choices for a site ... 88
Sites field descriptions ... 89
Initial topology administration ... 95
Overview for administering topology ... 95
Mutare Message Mirror™ ... 96
Adding the first application server ... 96
Adding additional application servers ... 97
Changing the storage server role ... 99
Configuring a cluster ... 99
Administering a load balancer in the Exchange Server CAS array ... 100
Topology field descriptions ... 102
Cluster field descriptions ... 103
Verifying the link to the AxC ... 103
Chapter 7: Managing servers ... 105
Storage servers ... 105
Adding a trusted server ... 105
Manage Trusted Servers field descriptions ... 106
Add Trusted Server field descriptions ... 106
Report of Trusted Servers field descriptions ... 107
Setting Messaging parameters ... 108
Privacy enforcement ... 108

Setting the privacy enforcement level for IMAP4 and POP3 clients ... 109
Configuring IMAP4 access ... 109
System Ports and Access field descriptions ... 110
Adding a network server ... 113
Manage Networked Servers field descriptions ... 114
Add Networked Machine field descriptions ... 114
Report of Network Servers field descriptions ... 117
Network Snapshot field descriptions ... 118
Report of Server Ranges field descriptions ... 119
Application servers ... 119
Dial Rules field descriptions ... 119
Dial Plan Handling Test field descriptions ... 121
Dial-Out Rules field descriptions ... 122
Dial-In Rules field descriptions ... 123
Fax overview ... 124
Nightly maintenance ... 124
Message recording ... 124
Configuring system parameters ... 125
System Parameters field descriptions ... 125
Changing the configuration of a cluster ... 130
Configuring storage capacity for offline call answering ... 130
External servers ... 131
Changing external SMTP hosts ... 131
Chapter 8: Managing users ... 133
User overview ... 133
User options for responding to messages ... 133
Manage local users ... 134
Adding users ... 134
Adding users from Active Directory ... 135
Changing user properties ... 136
Deleting users ... 137
Speech recognition ... 137
User Management field descriptions ... 138
User Management > Properties field descriptions ... 139
Configuring system policies ... 143
System Policies field descriptions ... 143
Manage info mailboxes ... 145
Info mailbox overview ... 145
Adding an info mailbox ... 146
Properties for New Info Mailbox field descriptions ... 146
Manage mailboxes ... 148
Adding a mailbox ... 148
Deleting a mailbox ... 149
Unlocking the voice mailbox account ... 149
Resetting the voice mailbox password ... 150
Changing the voice mailbox password ... 150
Manage remote users ... 151

Types of remote users ... 151
Addressing remote users ... 152
Remote updates ... 152
Setting up remote updates ... 153
Running a remote update manually ... 153
Request Remote Update field descriptions ... 154
Chapter 9: Class of Service ... 155
Class of Service overview ... 155
Adding a Class of Service ... 156
Changing a Class of Service ... 156
Deleting a Class of Service ... 157
Basic and Mainstream mailbox licensing ... 157
License status ... 158
Class of Service field descriptions ... 158
Adding mobile operators ... 165
Testing mail gateways ... 166
Mobile Operators field descriptions ... 167
Deleting broadcast messages ... 167
Chapter 10: Distribution lists ... 169
Enhanced-List Application overview ... 169
Implementing ELA ... 169
Creating a shadow mailbox ... 169
Configuring a shadow mailbox ... 170
System Mailboxes field descriptions ... 171
Adding a new ELA list ... 172
Manage Enhanced-Lists field descriptions ... 172
Create a New Enhanced-List field descriptions ... 173
Loading lists ... 175
Administering an ELA List ... 176
Sort Enhanced-List field descriptions ... 177
Report of Enhanced-Lists field descriptions ... 177
Managing enhanced-list members and administrators ... 178
Enhanced-List Membership and Administrators field descriptions ... 179
Enhanced-List Membership Report field descriptions ... 180
Chapter 11: Caller applications ... 181
Caller applications overview ... 181
Caller Applications Editor ... 181
System requirements ... 181
Containers ... 182
Prompts ... 182
Recording an audio prompt ... 183
Changing the .wav file format ... 183
Text-to-Speech prompts ... 183
Menus ... 184
Menu actions ... 184
Example menu ... 185
Schedules ... 187

Business schedules ... 187
Holiday schedules ... 187
Planning a caller application ... 188
Caller applications checklist ... 188
Worksheet for container properties ... 189
Worksheet for menus ... 189
Installing Caller Applications Editor ... 194
Changing the Caller Applications password ... 194
Working in Caller Applications Editor ... 195
Logging in to Caller Applications Editor ... 195
Creating containers ... 195
New Caller Application field descriptions ... 196
Creating menus ... 197
Creating business schedules ... 198
Creating holiday schedules ... 198
Assigning audio prompts to menus ... 199
Deploying a caller application ... 199
Chapter 12: Teletypewriter ... 201
Teletypewriter overview ... 201
Important information ... 202
Setting up a teletypewriter for your system and the user ... 202
Inform teletypewriter users about the login option ... 203
Ensure that teletypewriter users receive broadcast messages ... 203
Ensure voice quality ... 203
Chapter 13: Managing software ... 205
Viewing the currently installed software ... 205
Patch installation overview ... 205
Installing software ... 206
Verifying system installation ... 207
Installing advanced software ... 207
Deleting software packages ... 208
Chapter 14: Back up and restore ... 211
Back up and restore overview ... 211
Backing up system files ... 213
Backup Now field descriptions ... 214
Backing up System Platform ... 216
Backup field descriptions ... 217
Scheduled backups ... 217
Adding a new backup schedule ... 218
Changing a backup schedule ... 219
Deleting a backup schedule ... 219
Viewing backup history ... 220
Viewing backup logs ... 220
Backup Logs field descriptions ... 221
Performing a restore ... 221
View/Restore Data field descriptions ... 223
Viewing restore history ... 224

Storage space calculation ... 224
Restoring System Platform configuration information ... 225
System Platform restore field descriptions ... 225
Viewing System Platform restore history ... 226
Chapter 15: Alarms ... 227
Alarms overview ... 227
Alarm notifications ... 228
Viewing current alarms ... 229
Current Alarms field descriptions ... 229
Configuring certificate alarms ... 231
Certificate Alarms field descriptions ... 231
Viewing the alarm summary ... 232
Alarm Summary field descriptions ... 232
SNMP Traps ... 232
Configuring SNMP trap destinations ... 233
Configure SNMP trap destinations field descriptions ... 233
Changing an administered SNMP trap ... 235
Deleting an administered SNMP trap ... 235
SNMP filter administration ... 236
Adding an SNMP filter ... 237
Changing an SNMP filter ... 237
Deleting one or all SNMP filters ... 237
Add Filter field descriptions ... 238
Administering an SNMP Agent ... 239
SNMP Agents field descriptions ... 240
Viewing and changing the agent status ... 242
Sending a test trap ... 242
Chapter 16: Logs ... 243
Logs overview ... 243
Viewing the system logs ... 244
System Logs field descriptions ... 245
System log results ... 247
Storage server logs ... 252
Storage server logs overview ... 252
Viewing the administration history log ... 252
Administration History Log field descriptions ... 253
Administration History Log Results field descriptions ... 253
Viewing the administrators log ... 254
Administrator's Log field descriptions ... 254
Administrator's Log Results field descriptions ... 255
Viewing the alarm logs ... 256
Alarm Log field descriptions ... 256
Alarm Log Results field descriptions ... 258
Viewing the software management logs ... 259
Software Management Logs field descriptions ... 259
Viewing the maintenance logs ... 259
Maintenance Log field descriptions ... 260

Maintenance Log Results field descriptions ... 261
Viewing the Internet messaging logs ... 261
Internet Messaging Logs field descriptions ... 262
Viewing the ELA delivery failure logs ... 263
Enhanced-List Delivery Failure Log field descriptions ... 263
User activity logs ... 264
Configuring a user activity log ... 264
User Activity Log Configuration field descriptions ... 264
Running an activity log report ... 264
User Activity Log field descriptions ... 265
Application server logs ... 266
Application server logs overview ... 266
Configuring the log settings ... 266
Log Configuration field descriptions ... 267
Running the system log filter ... 267
System Log Filter field descriptions ... 268
Collecting the system log files ... 269
Collect System Log Files field descriptions ... 269
Viewing the call records ... 269
Accessing audit and ports usage files ... 270
Viewing the port usage report ... 271
Port Usage Report descriptions ... 271
Accessing diagnostics results ... 274
Sending logs to an external syslog server ... 275
Syslog Server field descriptions ... 275
Chapter 17: Reports ... 277
Reports overview ... 277
Report types ... 277
Viewing the local users report ... 278
Users (Local) field descriptions ... 278
Viewing the information mailboxes report ... 279
Information Mailboxes field descriptions ... 280
Viewing the remote users report ... 280
Remote Users field descriptions ... 281
Viewing the uninitialized mailboxes report ... 282
Uninitialized Mailboxes field descriptions ... 282
Viewing the login failures report ... 283
Login Failures field descriptions ... 284
Viewing the locked out users report ... 285
Locked Out Users field descriptions ... 285
Running the system evaluation report ... 286
Viewing the Internet messaging traffic ... 286
Internet Messaging Traffic field descriptions ... 287
Viewing the TCP/IP snapshot ... 288
Running the traffic measurement report ... 289
Messaging Measurements field descriptions ... 289
Viewing the login reports ... 290

Login Reports field descriptions ... 291
Chapter 18: Maintenance ... 293
Maintenance checklist ... 293
Application server ... 293
Storage server ... 295
Messaging database audit ... 300
Performing the voice messaging database audit ... 301
Messaging Database Audits (Storage) field descriptions ... 301
Audit History field descriptions ... 302
Running Audit ... 302
Verifying or restarting the LDAP processes ... 302
LDAP Status/Restart (Storage) field descriptions ... 303
Octel Aria migration ... 304
Importing Octel Aria data ... 304
Octel Aria Migration field descriptions ... 305
IMAP/SMTP administration ... 306
Administering general options ... 306
Internet Messaging: General Options and Settings field descriptions ... 306
Mail options ... 307
Configuring the mail options ... 307
Mail Options field descriptions ... 308
Verifying the IMAP/SMTP status ... 309
IMAP/SMTP status field descriptions ... 309
Voice Equipment Diagnostics ... 310
Busying out voice channels ... 310
Busyout of Voice Equipment field descriptions ... 311
Diagnosing the voice equipment ... 311
Diagnose Equipment field descriptions ... 313
Displaying the voice equipment status ... 313
Display Voice Equipment field descriptions ... 313
Releasing the voice channels ... 314
Release of Voice Equipment field descriptions ... 315
Security ... 315
Generating a certificate signing request ... 315
Certificate Signing Request - Form field descriptions ... 317
Downloading files ... 317
Download Files field descriptions ... 318
Trusted Certificates ... 319
Displaying a trusted certificate ... 319
Adding a trusted certificate ... 319
Deleting a trusted certificate ... 321
Copying a trusted certificate ... 321
Trusted Certificates field descriptions ... 322
Server/Application Certificates ... 322
Displaying a certificate ... 322
Adding a server and application certificate ... 323
Deleting a certificate ... 324

Copying a certificate ... 324
Server/Application Certificates field descriptions ... 325
Authentication File ... 325
Authentication File field descriptions ... 326
Firewall ... 327
Install Root Certificate using Internet Explorer ... 327
SSH Keys ... 328
SSH Keys field descriptions ... 328
Enabling or disabling services on the server ... 328
Role-Based Access Control ... 329
Using diagnostic tools ... 332
Testing the alarm origination ... 332
Testing the LDAP connection ... 333
Testing the SMTP connection ... 333
Internet Messaging: SMTP Connection Test field descriptions ... 333
Testing the POP3 connection ... 334
Internet Messaging: POP3 Connection Test field descriptions ... 334
Testing the IMAP4 connection ... 334
Internet Messaging: IMAP4 Connection Test field descriptions ... 335
Testing the mail delivery ... 335
Internet Messaging: Mail Delivery Test field descriptions ... 335
Testing the name server lookup ... 336
Test Name Server Lookup field descriptions ... 336
Name Server Lookup Results field descriptions ... 336
Running application server diagnostics ... 337
Diagnostics (Application) field descriptions ... 337
Ping ... 339
Using the ping command ... 339
Ping field descriptions ... 339
Ping results ... 340
Traceroute ... 341
Using the traceroute command ... 341
Traceroute field descriptions ... 342
Traceroute results ... 343
Netstat ... 344
Running the Netstat command ... 344
Netstat command field descriptions ... 345
Netstat results ... 346
Server information ... 348
Verifying the status of the application role ... 348
Monitoring voice channels in real time ... 349
Voice Channels (Application) field descriptions ... 350
Voice Channel Monitor field descriptions ... 350
Viewing the cache statistics ... 350
Monitor cache statistics ... 351
Advanced application server settings ... 352
Reload application server cache ... 352

System Operations field descriptions ... 352
Configuring the timeouts information ... 354
Timeouts field descriptions ... 355
Viewing the AxC address ... 356
AxC Address field descriptions ... 356
Configuring the miscellaneous information ... 357
Miscellaneous field descriptions ... 357
Enabling core file generation ... 358
Core Files field descriptions ... 359
Server configurations ... 359
Configuring the network settings ... 359
Network Configuration field descriptions ... 360
Static routes ... 360
Adding a static route ... 361
Deleting a network route ... 361
Static Route field descriptions ... 362
Viewing the display configurations ... 362
Display Configuration field descriptions ... 362
Server maintenance ... 363
Changing the IP address and hostname of the Messaging server ... 363
Manage updates ... 364
Manage Updates field descriptions ... 364
Viewing the status summary ... 365
Status Summary - Refresh Mode field descriptions ... 366
Viewing the process status ... 368
Process Status field descriptions ... 369
Process Status Results field descriptions ... 369
Server shutdown ... 372
Shutting down the server ... 373
Shutting down the application server as an emergency plan ... 373
Viewing the software version ... 374
Software Version field descriptions ... 374
Monitoring performance ... 375
Restart software ... 377
Messaging failover behavior ... 378
Failover experience ... 378
Chapter 19: Redundant Message Store ... 381
Mutare Message Mirror ... 381
Message store redundancy with duplicated application servers ... 381
Message store redundancy with shared application servers ... 385
Caveats ... 390
Planning and preconfigurations ... 391
Messaging Hardware and Software requirements ... 391
Mutare Message Mirror requirements ... 392
Configuration information ... 393
Checklists ... 394
Checklist for duplicated application server configuration ... 394

Checklist for shared application server configuration 412
Validating the configuration 429
Chapter 20: Troubleshooting 433
System cannot recognize the DTMF tones 433
System drops call while logging in to the mailbox 433
System displays an error while performing a backup 434
Application server does not recognize users 434
Message is sent successfully but MWI does not turn on 435
Message does not reach recipient 436
Fax troubleshooting 436
Appendix A: Changing the server role from storage and application to storage only 439
Index 443

Chapter 1: Introduction

Purpose

This document describes the administration of the Messaging system that includes administering of the application and storage servers, configuring sites and topology, managing servers, users, and software, using reports, and using diagnostic tools among other administration activities.

Intended audience

This document is intended for an administrator who needs to configure and maintain the Messaging system.

Document changes since last issue

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

Added new fields in the Telephony Integration and the Storage Destinations field descriptions.

Related resources

Documentation

You can download the documents you need from the Avaya Support website at http://support.avaya.com. In addition to the documentation listed here, you can download a zip file that is a compilation of the Avaya Aura® Messaging documentation library. You can install this library on a computer or on your corporate network.

The Avaya Support website also includes the latest information about product compatibility, ports, and Avaya Aura® Messaging releases.

Related topics:

Administration on page 16

Administration

Title	Description	Audience
Administering Avaya Aura® Messaging	Explains how to use the System Management Interface (SMI) to configure your servers, sites, and topology; use reports and diagnostic tools; manage software and users; and perform routine maintenance tasks. The content is available as SMI Help and as a PDF file.	Administrator
Job aid for Administering Avaya Aura® Messaging	This job aid is a subset of the administration guide and includes the following routine administration tasks: rebooting the system, checking alarms, adding and deleting mailboxes, getting performance indicators, and unlocking, resetting, and changing mailbox passwords.	Administrator
Avaya Aura® Messaging Alarms and Events	Describes system alarms, events, and repair procedures.	Administrator and support personnel

Training

You can get the following Messaging courses at https://www.avaya-learning.com. Enter the course code in the **Search** field and click **Go** to search for the course.

The course titles may differ from the titles shown below.

Course code	Course title
2U00230W	Avaya UC Messaging— Overview
2U00231W	Avaya UC Messaging— Heritage
2U00232W	Avaya UC Messaging— Avaya Aura® Messaging
2U00233O	Selling Avaya UC Messaging Learning Bytes
3U00141W	Designing UC Messaging— Avaya Aura® Messaging
5U00140E	Avaya Aura® Messaging Implementation and Support
5U00141E	Avaya Aura® Messaging Administration
ATI01674VEN	Avaya Aura® Messaging— Caller Applications

Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

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

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

Warranty

Avaya provides a 3-month limited warranty on Messaging. Detailed terms and conditions are contained in the sales agreement or other applicable documentation and establish the terms of the limited warranty. In addition, the standard warranty description and details for support during warranty are available on the Avaya Support website at http://support.avaya.com. See specifically *Avaya Global Software License Terms*.

Chapter 2: Preparing for Avaya Aura® Messaging

Prepare your network

Network overview

You must configure your IT infrastructure to allow:

- Inbound traffic flow to the Messaging server
- Outbound traffic flow from the Messaging server

To enable this traffic flow, ensure that your network Domain Name System (DNS) record includes the appropriate Messaging information.

For more information on the network topology and bandwidth requirements, see *Avaya Aura® Messaging Overview and Specification*.

DNS record

You can create a Canonical Name (CNAME) record for the Messaging server in DNS. A CNAME record is a type of resource record in DNS that specifies that the domain name is an alias of another canonical domain name. A CNAME record is simply a pointer to another A record. In case, you did not create A record, follow these guidelines when you create an alias:

- If you have a front-end or back-end topology, point the alias to the storage server .
- Use *avayamsg* as the alias. For example: *avayamsg.example.com*. Use this name for the Messaging documentation as a different name might confuse users.
- Ensure that your mail gateway:
  - Relays the fully qualified domain name (FQDN) for the storage server.
  - Sends messages to Internet domains.
  - Grants IP access to the storage server. Some mail gateways restrict IP access.

- Requires no SMTP authentication. Use IP-based restrictions for the mail gateway.

Prepare for Exchange forms

Exchange administration overview

The voice message form adds a dedicated toolbar to Microsoft Outlook. Use this toolbar to play voice messages and call the email sender from Outlook. To integrate Messaging with Outlook, you must:

- Verify that your Exchange server has the forms folders.
  - If the Exchange server does not have the forms folders, you must create the forms folders.
- Use Outlook to add the voice message forms to the forms folders on your Exchange server.

You can add the form to the system folder on any of the following Exchange servers:

- Exchange 2007
- Exchange 2010

System folders are hidden folders for internal Exchange System Management. In large organizations with specialized administration roles, the Exchange administrator completes these tasks.

Organizational Forms Library

An Organizational Forms Library is a repository for forms. You can have only one Organizational Forms Library for each language in an organization. You must publish a form to this library if you want to make the form available to everyone in your organization. For example, publish a form to report vacation time.

The library is stored on Microsoft Exchange Server. You must assign permissions to individuals to publish to Organizational Forms Library. You must provide permission to only some individuals or a department that manages the Exchange server.

Voice messaging form

The voice messaging form resembles the default email form, but gives users an interface for performing actions such as playing, stopping, or pausing voice messages, and calling the sender from Microsoft Office Outlook. The voice messaging form includes a notes field and the default media player configured on the system of the user.

The system displays the default media player and the notes field either in the preview pane when previewing a voice message or in a separate window when the user opens the voice

message. If you have not installed Microsoft Office Outlook on the client computer, users receive voice messages only as attachments in their client applications, and the voice messaging form is unavailable.

Note:

Messaging does not support Microsoft Office Outlook 2003 for voice messaging forms.

Supported languages

The voice messaging forms are available at `http://avayamsg/download/<VoiceMessagingFormFilename>` in the following languages. Replace *VoiceMessagingFormFilename* with the preferred file name.

Language	File name
Arabic	AvayaVoiceMessage_ar-SA.fdm
Brazilian Portuguese	AvayaVoiceMessage_pt-BR.fdm
Spanish	AvayaVoiceMessage_es-ES.fdm
Chinese	AvayaVoiceMessage_zh-CN.fdm
Dutch	AvayaVoiceMessage_nl-NL.fdm
French	AvayaVoiceMessage_fr-FR.fdm
German	AvayaVoiceMessage_de-DE.fdm
Italian	AvayaVoiceMessage_it-IT.fdm
Japanese	AvayaVoiceMessage_ja-JP.fdm
Korean	AvayaVoiceMessage_ko-KR.fdm
Polish	AvayaVoiceMessage_pl-PL.fdm
Russian	AvayaVoiceMessage_ru-RU.fdm
Latin American Spanish	AvayaVoiceMessage_es-XL.fdm
U.S. English	AvayaVoiceMessage_en-US.fdm

Organizational Forms Library

Add Organizational Forms Library to the system folder on any of the following Exchange servers:

- Exchange 2007
- Exchange 2010

For each Organization Forms Library, you must assign client permissions.

Related topics:

Adding Organizational Forms Library on page 22
Modifying Organizational Forms Library properties on page 22
Making Organizational Forms Library visible to Microsoft Office Outlook users on page 23

Adding Organizational Forms Library

Procedure

1. Open Exchange Management Shell.
2. To create a new folder for Organizational Forms Library, run the `New-PublicFolder -Path "\NON_IPM_SUBTREE\EFORMS REGISTRY" -Name "Organizational Forms Library` command.
   Exchange Management Shell creates a new public folder for Organizational Forms Library in the EFORMS REGISTRY folder.

Modifying Organizational Forms Library properties

Use this procedure to modify and export Exchange Server folder properties, export and import permissions and replica lists, enumerate items, gain access to mailboxes and other tasks. Perform these tasks through the ExFolders tool. This tool supports Exchange Server 2007 and 2010.

Before you begin

Download the ExFolders tool from the *Exchange 2010 SP1 (and later) ExFolders* page of the *Microsoft Technet* website at http://gallery.technet.microsoft.com/Exchange-2010-SP1-ExFolders-e6bfd405.

Ensure that you move the `ExFolders.exe` file to the `C:\Program Files\Microsoft\Exchange Server\V14\Bin`. If the `ExFolders.exe` file is located in a different folder, the ExFolders tool fails.

Procedure

1. Double-click the `Exfolders.exe` file.

   Note:

   - You must run the tool from an Exchange Server 2010 server.
   - If you are using the tool for the first time, ensure that you run the `.reg` file in the ExFolders compressed file before using the tool.

2. Click **File** > **Connect** > **Public Folders**.
3. Select **Global Catalog and Databases**.
4. Expand **System Folders** > **EFORMS REGISTRY**.
5. Right-click the public folder that you created for Organizational Forms Library and click **Property Editor**.
6. In the Name column, right-click **PR_URL_NAME** and select **Edit Value**.
7. In the Value box, type `/NON_IPM_SUBTREE/EFORMS REGISTRY` and click **OK**.
8. Close the ExFolders tool.

Making Organizational Forms Library visible to Microsoft Office Outlook users

Before you begin

Download the Microsoft Exchange Server MAPI Editor (MFCMAPI) tool from the *MFCMAPI* page of the CodePlex website at mfcmapi.codeplex.com. Ensure that you download the tool on a computer that is installed with the 64–bit version of Microsoft Office Outlook.

Caution:

Exercise caution when you use the MFCMAPI tool. Incorrect modifications might adversely affect the Microsoft Exchange Server administration.

About this task

You can make Organizational Forms Library visible to all Microsoft Office Outlook users using the MFCMAPI tool which uses the published APIs of Microsoft to provide access to MAPI stores through GUI.

Procedure

1. Open MFCMAPI.
2. Click **Session** > **Logon** and select your profile.
3. Click **Session Menu** > **Advanced Logon** > **Display Store Table**.
4. Click **MDB** > **Public Folder** > **Open Public Folder Store** and click **OK**.
   The MAPI editor opens the Public Folder Management Console.
5. Expand **Public Root** > **NON_IPM_SUBTREE** > **EFORMS REGISTRY** and select Organization Forms Library.
6. In the Property Name(s) column, click the **PR_URL_NAME** property.
7. Click **Property** > **Additional Properties** and click **Add**.

8. In Property Tag Editor, click **Select Property Tag**.
9. In Property Selector, click **PR_EFORMS_LOCALE_ID** and click **OK**.
10. To close Property Tag Editor, click **OK**.
11. To close Additional Properties, click **OK**.
12. To verify that the property is added, in the Public Folder Management Console, find the new **PR_EFORMS_LOCALE_ID** property in the **Property Name(s)** column.

    Tip:

    The icon of a new property is a red exclamation mark (!).
13. To open Property Editor, double-click **PR_EFORMS_LOCALE_ID**.
14. In the **Unsigned Decimal** box, type the locale ID that you want, for example, type `1033` for English, and click **OK**.
15. Close MFCMAPI.

Installing the voice message form

Before you begin

- You have a system folder on the Exchange server that contains one Organizational Forms Library for each language in a multilingual deployment.
- You have an account with client permissions for administering Organizational Forms Library.
- You have completed either of the following:
  - Configured the avayamsg A or CNAME record in DNS. For more information, see DNS record on page 19.
  - Recorded the host name or IP address of a Messaging server.

About this task

To install the voice message form on a computer that runs Outlook.

Procedure

1. Log in with the user account that has client permissions.

   Use the user account you created in the `EFORMS REGISTRY`.
2. In a Web browser, run the URL: **http://avayamsg/download/*<VoiceMessagingFormFilename>*** and save the form to a temporary location on your hard drive.

Replace *VoiceMessagingFormFilename* with the appropriate filename. See Supported languages on page 21 for a list of file names.

3. For each language that you want to deploy, repeat Step 2 .
4. Open Outlook and select **Tools** > **Options** > **Other** > **Advanced Options...** > **Custom Forms**.

   For Outlook 2010, you must navigate to **File** > **Options** > **Advanced** > **Custom Forms**.
5. In the Options dialog box, click **Manage Forms**.
   In the Forms Manager dialog box, the system displays *Personal Form* in the right pane where you created the form.

   If you have a multilingual deployment, ensure that the language for Organizational Forms Library and the voice message form match.
6. In the Forms Manager dialog box, click **Install**.
7. In the **Files of type** field, select **Form Message (*.fdm)**.
8. Navigate to the voice message form file that you downloaded in Step 2. For example, `AvayaVoiceMessage_en-US.fdm`.
9. Click **Open** to install the form file.

   If the library already contains a version of this voice message form, the system displays a confirmation dialog box.

   To replace the existing form with this version, click **Yes**.
10. In **Form Properties**, click **OK**.
11. Set the folder so that the form takes effect.
12. In the right pane, select **Avaya Voice Message** in *Personal Form*.
13. To copy the voice message form into your forms library, click **Copy** .

    If you are deploying multiple languages, repeat Step 8 through Step 14 for each language form.
14. Click **Close**.
15. Click **OK** three times to close the dialog boxes.
    When a user opens a voice message, the appropriate voice messaging form downloads automatically.

Chapter 3: Getting started with Avaya Aura® Messaging

Administration overview

System Management Interface

System Management Interface (SMI) is the single point of access for your Messaging system and the license server. You can open SMI from any standard Web browser from anywhere within the firewall of your organization.

SMI has three interfaces:

- The licensing administration interface to view the status of the server license.
- The Messaging administration interface to gain access to administration, diagnostic, and reporting tools to set up, manage, and maintain your Messaging system.

  In addition to monitoring system status, you can also use the Messaging administration interface to administer:

  - Server roles, trusted and hosted servers, sites, and topology
  - Features like Auto Attendant and call transfer
  - IMAP and SMTP
  - Users and CoS
- The server administration interface to configure, maintain, and troubleshoot Messaging servers.

Administration passwords

Password security

To minimize the risk of unauthorized access to 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.

Login Account Policy

Use the Login Account Policy Web page to establish policies for administrator logins. This page displays the current active values for each parameter.

You cannot use the Login Account Policy Web page to administer logins whose credentials are maintained in an external AAA server. This includes SecurID and SafeWord based logins. You must perform administration of these logins using the *root* login using standard Linux commands.

Note:

Use the Login Account Policy Web page to set global policy for all logins created using the Web interface. The Web interface does not support the ability to grant exceptions.

For example, you administer a policy for users to change the passwords every 90 days. To create a login not subject to this rule, you must create the login through the *root* login using standard Linux commands.

Viewing the login account policy

Procedure

On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Login Account Policy**.
The system displays the Login Account Policy Web page.

Login Account Policy field descriptions

Name	Description
Credential Expiration Parameters: This section displays the current expiration policy values for local passwords. Changing these parameter values affects future behavior of the system and does not affect the existing logins.	
The maximum number of days a password may be used (PASS_MAX_DAYS)	The values range from 1 through 99999.
The minimum number of days allowed between password changes (PASS_MIN_DAYS)	The values range from 0 through 99999.
The number of days a warning is given before a password expires (PASS_WARN_AGE)	The values range from 0 through 30.
The number of days after a password expires to lock the account (INACTIVE; 0 = immediate, 99999 = never)	The values range from 0 through 99999.
Failed Login Response: This section displays the current active values for each failed login response parameter. Changing these values immediately affects failed login response behavior.	
Enable account lock out parameters (PAM Tally)	You can ignore the remaining parameters if you clear the check box.
Lock out account after the following number of unsuccessful attempts (DENY)	The values range from 1 through 9.
Automatically unlock a locked account after the following number of seconds (UNLOCK_TIME)	The values range from 1 through 99999.
Reset the failed attempt counter after last failed attempt (UNLOCK_RESET)	Click **yes** to reset the failed attempt counter after last failed attempt.

Name	Description
	Click **no** to leave the failed attempt counter unchanged.

Adding a privileged administrator login

About this task

You must add a privileged administrator login that is a member of the SUSERS group. This login has the most advanced administrative access in the system with the exception of the root login. This ensures system security and prevents unauthorized access to your Messaging system.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Administrator Accounts**.
2. In the **Select Action** area, select **Add Login**.
3. Select **Privileged Administrator**.

   For more information, see Administrator Accounts field descriptions on page 31.
4. Click **Submit**.

   The system displays the Administrator Accounts -- Add Login: Privileged Administrator Web page.
5. Enter information in the following fields:
   - **Login name**
   - **Date after which account is disabled-blank to ignore (YYYY-MM-DD)**: Clear this field
   - **Enter password or key**
   - **Re-enter password or key**

   Note:

   Do not change other default values in the Administrator Accounts -- Add Login: Privileged Administrator Web page.
6. Click **Submit**.

   The system creates the privileged administrator login.
7. Click **Continue** to go back to the Administrator Accounts Web page.

Comments? infodev@avaya.com

Changing an administrator password

Each account has a default password. You must change these default passwords the first time you log in to the Messaging system.

Use the Administrator Accounts Web page to add, delete, or change administrator logins and Linux groups.

Procedure

1. Use the privileged administrator login and password.
   If the privileged administrator login does not exist, you must create a privileged administrator account that is part of the *susers* group.
2. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Administrator Accounts**.
3. Select **Change Login** and select the login account from the list.
4. Click **Submit**.
5. Enter the new password in the **Enter password or key** field.
6. Enter the password again in the **Re-enter password or key** field.
7. Click **Submit**.
   The system changes the login password.

Administrator Accounts field descriptions

You must use REMOTE logins only to establish a PPP session with the Messaging server through the modem interface. You must not use REMOTE logins to access a shell, a SAT, CDR records, or the Web pages.

You must use ADMINISTRATIVE logins to gain access to a shell, a SAT or the Web pages but not to establish a PPP session or to acquire CDR records.

You must use a CDR login specifically to retrieve CDR records stored on the server. You must not use the CDR login for any other purpose.

- REMOTE logins: When creating a REMOTE login, you must specify the login name, but you must not specify group membership or select a shell. You must not change a REMOTE login to an ADMINISTRATIVE or CDR type of login. You must delete a REMOTE login and create a new login.
- CDR logins: When creating a CDR login, you must enter CDR_user as the login group.
- ADMINISTRATIVE logins: The system controls the access provided to an ADMINISTRATIVE login by checking whether the system assigned a shell and access

profile to the login. To assign the access profile, you must assign an *additional group* to the login.

Field	Description
Select Action	
Add Login	Select this option and select the type of login you want to add. The options are: • **Privileged Administrator** • **Unprivileged Administrator** • **Web Access Only** • **CDR Access Only** • **Business Partner Login (dadmin)** • **Business Partner Craft Login** • **Custom Login**
Change Login	Select this option and select a login from the drop-down list.
Remove Login	Select this option and select a login from the drop-down list.
Lock/Unlock Login	Select this option and select a login from the drop-down list.
Add Group	Select this option to add a group.
Remove Group	Select this option and select a group from the drop-down list.

Checklist for administrators

The following components are required for the proper functioning of the Messaging system on your IT infrastructure:

- Network
- Exchange server (optional)
- Telephony server
- Messaging storage role
- Messaging application role
- Messaging sites and topology

The following table describes the initial administration tasks, the administrator who performs these tasks, and the component required by the administrator to perform and complete the tasks.

Since, IT responsibilities in large organizations are divided among different individuals, each chapter in the table contains the necessary information required by a specific administrator.

You must complete the chapters in the following sequence:

				Location		
No.	**Task**	**Chapter number**	**Administrator type**	**Single-server systems**	**Front-end / Back-end systems**	✔
1	Prepare the network	Chapter 1	Network administrator	—	—	
2	Load the Avaya voice messaging forms onto the Exchange server	Chapter 1	Exchange administrator	Exchange server	Exchange server	
3	Prepare the telephony server	*Supported and Unsupported Avaya Aura Messaging Integrations* on http://support.avaya.com/	Switch administrator	Telephony server	Single site: Telephony server Multisite: *Each* telephony server	
4	Set up the storage role	Chapter 3	Messaging administrator	Single server	Storage server	
5	Set up the application role	Chapter 4	Messaging administrator	Single server	Each application server	
6	Set up sites and topology	Chapter 5	Messaging administrator	Single server	Storage server	

Logging in to Messaging

About this task

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

Procedure

1. Open a compatible Web browser on your computer.
2. Depending on the server configuration, choose one of the following options:

Options	Description
Access by System Platform Web Console	• Log on to the System Platform Web Console. • Click **Virtual Machine Management** > **Manage**. The system displays the Virtual Machine List page. • Click the **Manage Virtual Machine** wrench icon to select the *msg* virtual machine.
LAN access by IP address	To log on to the corporate LAN, type the unique IP address of the Messaging server in the standard dotted-decimal notation, For example, `http://192.152.254.201`.
LAN access by host name	To log on using the corporate LAN that includes a DNS server administered with the name of the host, type the host name. For example, `http://avayamsg.example.com`.
Laptop access by IP address	To log on using the services port from a directly-connected laptop, type the unique IP address of the Messaging server in standard dotted-decimal notation. For example, `http://192.152.254.201`.

   If your browser does not have a valid security certificate, the system will display a warning screen and instructions to load the security certificate. If you are certain that your connection is secure, accept the server security certificate to gain access to the Logon screen. If you plan to use this computer and browser to access this or other Avaya servers again, install root certificate on your computer. The Root Certificate establishes Avaya Inc. as a trusted Certificate Authority (CA).
3. Click **Continue**.
   The system displays the Logon screen.
4. Click **Logon**.
5. Click **Logon**.

   After successful authentication, the system displays the Messaging SMI home page.

Logging out

Procedure

1. On any SMI page, click **Log Off**.
   The system displays a confirmation page.
2. Click **Log Off** to log out from the SMI.
   The system displays the Logon screen.

Chapter 4: Initial administration of the storage role

Initial administration checklist for the storage role

Use the following checklist as a guide for setting up a storage role for the first time. In large organizations with specialized administration roles, the Messaging administrator usually completes these tasks.

On the server running the storage role, perform the tasks in the following sequence:

No.	SMI page	References	✔
1	Server Date/Time	Verifying the system clock on page 38	
2	Change LDAP Password (Storage)	Changing the LDAP root password on page 39	
3	System Status (Storage)	Verifying the status of the storage role on page 40	
4	External Hosts	Administering the external SMTP host on page 41	
5	Mail Options	Adding a mailbox gateway on page 42	
6	Edit Networked Machine	Setting the length of mailbox numbers on page 43	
7	Properties for New User	Adding the postmaster mailbox on page 43	
8	System Mailboxes	Configuring the postmaster mailbox number on page 45	
9	Storage Destinations	Configuring a storage destination on page 52	
10	Properties for New User	Selecting a storage destination on page 55	

Verifying the system clock

In Messaging, you can perform certain time-dependent tasks with the use of the Linux system clock. For example, you can place a time stamp on voice messages and schedule a backup of critical system data.

When you install the system, the clock is set. However, check the clock when you administer your storage server initially. You must also check the clock every month and during a change in Daylight Savings Time.

Tip:

Use a Network Time Protocol (NTP) server to maintain accurate system time.

Warning:

If there is a time difference between the storage server and the application servers, the time difference might cause problems with message delivery and replication between the servers.

Before you begin

Ensure Messaging is running by clicking on the **Administration** menu, and clicking **Messaging** > **Utilities** > **Start Messaging**. If Messaging is running, the system displays the `Messaging is already started` message.

Procedure

On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Server Date/Time**.
The system displays the current date, time, and timezone.

For information on changing the system time, see *Administering Avaya Aura® System Platform*.

Note:

If you change the system time, you must restart Messaging for the changes to take effect. For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Changing the LDAP root password

Messaging uses the LDAP root password for internal LDAP processing. External LDAP clients, networked computers, and trusted servers do not use the LDAP root password.

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **Stop Messaging**. The system displays the Stop Messaging Software Web page.
2. If you want to initiate a shutdown, click **Stop**.
   The Stop Messaging Software Web page refreshes periodically during the shutdown routine and displays a brief status message after **Stop Messaging info.**

   After the Messaging software stops completely, the system displays the *Stop of Messaging completed* message.
3. Click **OK**.
4. On the **Administration** menu, click **Messaging** > **Utilities** > **Change LDAP Password (Storage)**.
5. Select **yes** or **no** from the **Change default LDAP Root Password?** drop-down list.
6. Enter the old password in the **Old Password** field.

   If you are changing the default LDAP Root Password for the first time, leave this field blank.
7. Enter the new password in the **New Password** field.
8. Enter the new password again in the **Confirm New Password** field.
9. Click **Save**.
10. On the **Administration** menu, click **Messaging** > **Utilities** > **Start Messaging**. The system displays the Start Messaging Software Web page.

    The Start Messaging Software Web page refreshes periodically during the startup routine and displays a brief status message after **Start Messaging information**.

    After the Messaging software starts completely, the system displays the *Start of Messaging completed* message.
11. Click **OK**.

Verifying the status of the storage role

Access the System Status (Storage) Web page whenever you want to confirm that Messaging is running. You can also verify that the following functions of the storage role are operational:

- Voice mail.
- Each software module enabled by you. For example, Enhanced-List Administration, Internet Messaging, and Message Networking.
- LDAP processes.
- The number of hours of speech that are available. Use these figures to determine if the system has sufficient space for recording voice messages.

Procedure

On the **Administration** menu, click **Messaging** > **Server Information** > **System Status (Storage)**.

For the status of the application role, see Verifying the status of the application role on page 348.

Example

The System Status (Storage) Web page displays the following information.

```
System status of VM

MessageCore IN SERVICE

System status of ela

/ela/registration/sys_stat/bin/status: The enhanced lists software is running...

System status of iim

Internet Messaging is currently: Running
Percent of media space in use (contains queues): 7.0%
Number of incoming messages in queue: 0
Number of outgoing messages in queue: 0
Number of SMTP receive sessions running: 0
Number of SMTP send sessions running: 0
Number of POP3 sessions running: 0

System status of ldapolv3

-------------------------------------------------------
----- LDAP processes -----
-------------------------------------------------------
LDAP internal server (slapd): UP
LDAP front end server (Ldapfe): UP
LDAP Corporate LAN server (Ldapcorp): UP
-------------------------------------------------------
----- Corporate LAN LDAP Access -----
-------------------------------------------------------
```

```
LDAP authenticated access on the Corporate LAN: UP
LDAP anonymous access on the Corporate LAN: UP

System status of mtce

Begin System Verification Checks -
File System Capacity Check Passed
IPC queue check passed

System status of vs

Voice System is Up
Available Hours of Speech 2102
Used Hours of Speech 205
Maximum Hours of Speech 2307
Number of Available Text-to-Speech Sessions 4
```

Enable outbound SMTP based traffic

Administering the external SMTP host

In Messaging, you can forward the following by using an external SMTP relay host:

- Text notifications and email notifications
- Email fax messages as file attachments
- Outbound voice messages

You can enable this function by configuring the mail gateway on the External Hosts Web page.

Note:

You must configure the receive connector of the external SMTP host to accept connections and messages from Messaging.

Before you begin

Ensure Messaging is running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Storage)** > **External Hosts**.
2. Click **Add**.
3. Enter the **IP address**, **Host Name**, and **Alias** of the external SMTP Server. Configuring the **Alias** is optional.

4. Click **Save**.

Add a New External Host field descriptions

Name	Description
IP Address	The IP address of the external SMTP server.
Host Name	The host name of the external SMTP server.
Alias	The alias of the external SMTP server. This field is optional.

Adding a mailbox gateway

Use Messaging to add a mailbox gateway to connect to other mail systems and send text messages from the storage server. For more information on network configuration requirements, see Network overview on page 19.

Procedure

1. On the **Administration** menu, click **Messaging** > **IMAP/SMTP Settings (Storage)** > **Mail Options**.
2. In the **Mailbox Gateway Machine Name** field, select the host name that you entered in Administering the external SMTP host on page 41.
3. Keep the **Server Alias** field blank.

   For more information, see Mail Options field descriptions on page 308.
4. Click **Save**.

Next steps

Identify the length and the range of valid digits required for accessing a mailbox. See Setting the length of mailbox numbers on page 43.

Setting the length of mailbox numbers

Before you begin

Ensure Messaging is running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Storage)** > **Networked Servers**.
2. On the Manage Networked Servers Web page, select the server and then click **Edit the Selected Networked Server**.
3. In the **Mailbox Number Length** field, enter a number that corresponds to the length of the mailbox extension used by your system.

   This is the length of the long/global mailbox number.
4. In the **MAILBOX NUMBER RANGES** area, enter the prefix and the range of mailbox numbers for Messaging.

   Enter a range of numbers that conforms to the number you selected in the **Mailbox Number Length** field.

   For example, if you selected 5 in the list, then enter a 5-digit number. If you selected 8, then enter an 8-digit number.

   Unless your organization has a specific reason for excluding some ranges, start with 1 with the appropriate number of leading zeros, and end with the highest possible number.

   The following example displays the range for a 5-digit mailbox number:

   - **Starting Mailbox Number**: `00001`
   - **Ending Mailbox Number**: `99999`

   For more information, see Add Networked Machine field descriptions on page 114.
5. Click **Save**.

Next steps

See Adding the postmaster mailbox on page 43.

Adding the postmaster mailbox

The postmaster is responsible for managing the emails for a site. The postmaster mailbox is a system-wide mailbox set aside for the postmaster. This mailbox is an internal system mailbox

integral to the operation of the Messaging system. Use these instructions to create a postmaster mailbox.

Before you begin

Ensure Messaging is running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. In the **Add User / Info Mailbox** area, click **Add** to add a new user.
3. On the User Management > Properties for New User Web page, complete the following fields:
   - In the **Last name** field, enter `postmaster`.
   - In the **Mailbox number** field, enter a unique mailbox number for the postmaster.
   - In the **Extension** field, enter the extension of the postmaster.

   The length of the mailbox number and extension must match the length that you specified in Setting the length of mailbox numbers on page 43.
4. Set **MWI enabled** to **No**.
5. Turn off the following defaults:
   - **Include in Auto Attendant directory**
   - **User must change voice messaging password at next logon**
6. Complete the following password fields. For more information, see User Management Properties field descriptions on page 139 for setting passwords:
   - **New password**
   - **Confirm password**
7. Click **Save**.
   The system creates a site-wide mailbox.

Next steps

- Define the mailbox that you just created as the postmaster mailbox. See Configuring the postmaster mailbox number on page 45.
- Create a new CoS for the postmaster with the mailbox size set at the maximum. For more information on creating a CoS with a maximum storage space, see Adding a Class of Service on page 156.

Configuring the postmaster mailbox number

After you create a mailbox for the postmaster, you must identify the mailbox as a postmaster mailbox.

Before you begin

Ensure that:

- You have created a mailbox for the postmaster. See Adding the postmaster mailbox on page 43.
- Messaging is running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Mailboxes**.
2. In the **Internet Postmaster Mailbox Number** field, enter the postmaster mailbox number.
3. Click **Save**.

   The system does not count the postmaster mailbox that you created against the total number of user licenses that your organization has purchased.

Next steps

Configure flexible storage. See Flexible storage on page 45.

Flexible storage

Using Messaging, you can configure multiple storage destination types for your Messaging system. You can use the following storage destinations to store your voice messages.

- Avaya message store: This is a built-in storage. To set up a storage role, see Initial administration checklist for the storage role on page 37.
- Microsoft Exchange 2007 or 2010: To configure Exchange as your storage destination, see Configuring a storage destination on page 52.

You can designate a storage server on a per user basis, allowing for a mixed environment of Avaya message store and Microsoft Exchange email servers.

The time setting on the application servers in the Messaging system and the configured storage server must be in synchronization. Even if the servers are in different time zones, the timestamps in UTC must match.

Hence, even if the time difference between the storage server and the Messaging server is only a few seconds in UTC equivalent, the Messaging system suppresses the outcall notifications on the messages.

Microsoft Exchange

Messaging supports either Microsoft Exchange 2007 or Microsoft Exchange 2010 as the message store. Messaging does not support Exchange Online. Messaging supports Active Directory provisioning.

You can use the Active Directory look-up utility to import user data into the Messaging directory. From the Active Directory, you can source user properties, such as mailbox, extension, and site information, based on the work phone data in Active Directory. Using the existing Active Directory means the most relevant user data, such as name or telephone numbers, is available for use by Messaging.

Configure the minimum required service account permissions

Depending on your storage destination, you must configure the following:

- *Avaya message store*: You do not need to perform any configuration.
- *Exchange 2007 or Exchange 2010*: For Exchange, the service account is a normal Active Directory Domain User account with an Exchange mailbox. You must provide Exchange Impersonation permissions to the account. Exchange Impersonation enables a caller to impersonate a given account so that a caller can perform operations by using the permissions that are associated with the impersonated account instead of the permissions that are associated with the account of the caller.

Creating the Messaging service account

Procedure

1. Open Exchange Management Console and select **Recipient Configuration**.
2. In the **Action** pane, click **New Mailbox**.
3. For **Mailbox Type**, choose **User Mailbox**.
4. For **User Type**, choose **New User**.
5. Complete the **User Information** fields.

   Use a site or location specific naming convention for the account name. For example, *AuraMsgSvcAcctSiteA*.
6. Complete the **Mailbox Settings** fields as needed, and click **Next**.
7. Complete the **Archive Settings** fields as needed, and click **Next**.
8. On the Summary screen, click **New** and verify that the system successfully created the mailbox.

9. Open Active Directory Users and Computers.
10. Locate your newly created service account, and right-click and select **properties**.
11. Click the **Account** tab and ensure that the **Password never expires** check box is selected.
12. In the **Member Of** tab, ensure your service account is *not* a member of any administrative group.

Configuring impersonation permissions for Exchange 2007

For each Exchange Server in the organization that functions as a *Client Access Server* (CAS), you must provide the ms-Exch-EPI-Impersonation Active Directory extended permission to the service account on the *Server* object of Exchange Server in Active Directory.

You must provide the ms-Exch-EPI-May-Impersonate extended permission to the Exchange store objects hosting Messaging users.

Note:

The service account that you use must not be a member of any Administrative Group, for example, Domain Admins, because the system explicitly denies these permissions for these groups.

Usually, you must provide the permission using the Add-ADPermission cmdlet on Exchange Management Shell, although you can also use Active Directory Sites and Services or Active Directory Users and Computers.

Note:

To complete the permission assignments, use an account with Domain Administrator credentials as well as administrative credentials for the computers on which you have installed the Exchange 2007 Client Access Server roles.

Procedure

1. Open Exchange Management Shell.
2. Use the Add-ADPermission cmdlet to assign ms-Exch-EPI-Impersonation permission for user accounts. The following cmdlet syntax grants the service account permission to impersonate all accounts for each Client Access Server. Replace *AuraMsgSvcAcctSiteA* in the following cmdlet with your Messaging Service Account: `Get-ExchangeServer | where {$_.IsClientAccessServer -eq $TRUE} | ForEach-Object {Add-ADPermission -Identity $_.distinguishedname -User (Get-User -Identity AuraMsgSvcAcctSiteA | select-object).identity -extendedRight ms-Exch-EPI-Impersonation}`

3. Use the Add-ADPermission cmdlet to assign the ms-Exch-EPI-May-Impersonate permission for Exchange Store objects on each Exchange Server hosting Avaya users. Replace *AuraMsgSvcAcctSiteA* in the following cmdlet with your Messaging Service Account: `Get-MailboxDatabase | ForEach-Object {Add-ADPermission -Identity $_.DistinguishedName -User AuraMsgSvcAcctSiteA -ExtendedRights ms-Exch-EPI-May-Impersonate}`

   Important:

   You must run the above command again after creating new mailbox databases that will host Avaya users.

   For more information, see the *Microsoft Exchange Server* website.

Configuring impersonation permissions for Exchange 2010

Microsoft Exchange Server 2010 uses Role-Based Access Control (RBAC) to assign Exchange Impersonation to accounts. You can provide Exchange Impersonation to the Messaging service account for all users in the organization or a specific group of users by creating a Management Scope with a specific Recipient Restrictions Filter.

Note:

To complete the permission assignments, use an account with Domain Administrator credentials or other credentials with the permission to create and assign Roles and Scopes, administrative credentials for the computers on which you have installed the Exchange 2010 Client Access Server roles, and Remote PowerShell installed on the computer used to run the commands.

Procedure

1. Open Exchange Management Shell.
2. Use the `New-ManagementRoleAsignment` cmdlet to assign `ms-Exch-EPI-Impersonation` permission for user accounts, which assigns Exchange Impersonation permission for all users to the Service Account. Replace *AuraMsgSvcAcctSiteA* in the following cmdlet with your Messaging Service Account: `New-ManagementRoleAssignment -Name:"Avaya Impersonation Role" -Role:ApplicationImpersonation -User:AuraMsgSvcAcctSiteA`

   For more information, see the *Microsoft Exchange Server* website.

Enabling the basic authentication for Exchange 2007 running Windows server 2003

Procedure

1. Click **Administrative Tools** > **Internet Information Services**.
2. Click **Web Sites** > **Default Web Site**.
3. Right click either the Exchange or Exchweb directory folders, and click **Properties**.
4. Click the **Directory Security** tab.
5. From the **Authentication and access control** heading, click **Edit**.
6. From the **Authenticated Access** section, select the following:
   a. Basic Authentication (password is sent in clear text)
   b. Integrated Windows authentication
7. Click **OK**.

Enabling the basic authentication for Exchange 2010 running Windows server 2008

Procedure

1. Open the **Exchange Management Console** and select the server.
2. Click **Server Configuration** > **Client Access**.
3. Select the server hosting the Outlook Web App virtual directory, and then click the **Outlook Web App** tab.
4. In the work pane, select the virtual directory, and then click **Properties**.
5. Click the **Authentication** tab.
6. From the **Use one or more standard authentication methods** heading, select the following:
   a. Basic Authentication (password is sent in clear text)
   b. Integrated Windows authentication
7. Restart IIS for the changes to take effect.

Granting the relay permission to anonymous connections for exchange 2007

Procedure

1. Open the **Exchange Management Console**.
2. In the console tree, click **Server Configuration** > **Hub Transport**.
3. In the result pane, select the server, and then click the **Receive Connectors** tab.
4. In the action pane, click **New Receive Connector**.
   The New SMTP Receive Connector wizard starts.
5. On the Introduction page, follow these steps:
   a. In the **Name:** field, type a meaningful name for this connector.
   b. In the **Select the intended use for this connector:** field, select **Custom**.
   c. Click **Next**.
6. On the Local network settings page, follow these steps:
   a. Select the **All Available** entry, and then click the cross icon.
   b. Click **Add**.
   c. In the **Add Receive Connector Binding** dialog box, select **Specify an IP address**.
   d. On the Local network settings page, in the **Port** field, enter **25**.
   e. Click **OK**.
   f. Click **Next**.
7. On the Remote Network settings page, follow these steps:
   a. Select the **0.0.0.0 - 255.255.255.255** entry, and then click the cross icon.
   b. Click **Add**.
   c. Enter the IP address or IP address range for the remote messaging server or servers to relay mail on this server.
   d. Click **OK**.
   e. Click **Next**.
8. On the New Connector page, review the configuration summary for the connector.
   - To change the settings, click **Back**.
   - To create the Receive connector by using the settings in the configuration summary, click **New**.
9. On the Completion page, click **Finish**.
10. In the work pane, select the Receive connector that you created.
11. Under the name of the Receive connector in the action pane, click **Properties**.
12. From the **Permission Groups** tab, select **Anonymous users**.

13. Click **OK**.

Granting the relay permission to anonymous connections for Exchange 2010

Procedure

1. Open the **Exchange Management Console**.
2. In the console tree, click **Server Configuration** > **Hub Transport**.
3. In the result pane, select the server, and then click the **Receive Connectors** tab.
4. In the action pane, click **New Receive Connector**.
   The New SMTP Receive Connector wizard starts.
5. On the Introduction page, follow these steps:
   a. In the **Name:** field, type a meaningful name for this connector.
   b. In the **Select the intended use for this connector:** field, select **Custom**.
   c. Click **Next**.
6. On the Local network settings page, follow these steps:
   a. Select the **All AvailableIPv4** entry, and then click the cross icon.
   b. Click **Add**.
   c. In the **Add Receive Connector Binding** dialog box, select **Specify an IP address**.
   d. On the Local network settings page, in the **Port** field, enter **25**.
   e. Click **OK**.
   f. Leave the **Specify the FQDN this connector will provide in response to HELO or EHLO** field blank.
   g. Click **Next**.
7. On the Remote Network settings page, follow these steps:
   a. Select the **0.0.0.0 - 255.255.255.255** entry, and then click the cross icon.
   b. Click **Add**.
   c. Enter the IP address or IP address range for the remote messaging server or servers to relay mail on this server.
   d. Click **OK**.
   e. Click **Next**.
8. On the New Connector page, review the configuration summary for the connector.
   - To change the settings, click **Back**.
   - To create the Receive connector by using the settings in the configuration summary, click **New**.

9. On the Completion page, click **Finish**.
10. In the work pane, select the Receive connector that you created.
11. Under the name of the Receive connector in the action pane, click **Properties**.
12. From the **Permission Groups** tab, select **Anonymous users**.
13. Click **OK**.

Configure Exchange Web Services

If you are using Microsoft Exchange as your storage destination, you must configure Exchange Web Services (EWS) to ignore client certificates. EWS provides the functionality to enable client applications to communicate with the Exchange server. EWS provides access to almost all data that is available through Microsoft Office Outlook.

By ignoring client certificates, any system can establish a connection to the EWS component and after authentication access the EWS component. For more information, see the *Microsoft Exchange Server* website.

Configuring a storage destination

You must perform this task if you plan to use Microsoft Exchange as your storage destination. The Avaya message store is automatically used and no further action is required on this Web page to use the Avaya message store.

Before you begin

Configure the mail host. For more information, see Adding a mailbox gateway on page 42.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Storage Destinations**.
   The system displays the Storage Destinations Web page.
2. Enter the appropriate information in the fields to define the required service account.
   For more information, see Storage Destinations field descriptions on page 53.
3. Click **Save**.
   The Messaging system:
   - Tries to log in to the account.
   - Checks that a corresponding mailbox has been created for that account.

If either test fails, then the system displays an error.

External storage destinations require specific settings on the System Ports and Access Web page. If you enable Exchange as your message store in Step 2 and save the changes, the system displays a message and sets the value in the:

- **Privacy Enforcement Level** field to *Email*
- **Automatic Mail Forwarding** field to *yes*

4. Click **OK**.
5. If the storage properties are saved, you need to restart Messaging for the changes to take effect.

   For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Storage Destinations field descriptions

Name	Description
Avaya Message Store	
To configure the Avaya message store, you must configure various storage related pages in the Messaging SMI. For more information, see Initial administration checklist for the storage role on page 37.	
Microsoft Exchange	
Enable	Enable the Exchange store and the fields in this section.
Service account	The user principal name (UPN) for the Exchange service account. For example, svc@domain.nnn. Messaging uses EWS to access the mailbox store and this is dependent on a single service account that can access the messages itself.
Password	The password for the Exchange service account.
Domain	The domain name for the Exchange service account.
Use Autodiscover service	Use the Auto Discovery service within Exchange to locate the email server that actually hosts the mailbox.

Name	Description
	If you select this check box and the **Storage destination** field on the User Properties Web page is Microsoft Exchange, then the system automatically populates the **Exchange server FQDN** field on the User Properties Web page after you click **Save** on that page. By default, this check box is selected.
Autodiscover	The Auto Discovery URL. For example, https://autodiscover.avaya.com/Autodiscover/Autodiscover.xml.
Use predefined Global Catalog server	The option to use a specific Global Catalog server. If you select this check box, you can administer a specific Global Catalog Server in **Global Catalog FQDN**. By default, Messaging automatically discovers the Global Catalog server. If the Global Catalog server and Exchange Server are administered in the same site as Microsoft Office Outlook, you do not need to specify a Global Catalog server.
Global Catalog FQDN	FQDN of the Global Catalog server such as exchange.aam02.mera.ru.
VMware Zimbra	Messaging does not support Zimbra as a storage destination in R6.2. Messaging displays the VMware Zimbra section only if you enabled Zimbra as a storage destination during the previous release.
Enable	Enable the Zimbra store and the fields in this section.
Service account	The Zimbra service account name. Configure this account as the global administrator in the Zimbra Administration Console.
Password	The password for the Zimbra service account.
Server name	The Zimbra server host name or IP address.
Admin service port	The administration service port.

Selecting a storage destination

If you configure a storage destination using the Storage Destinations Web page, then the system displays the **Storage destination** drop-down list on the User Management > Properties Web page.

Caution:

If you change the storage destination for an existing user, the existing voice messages will remain in their original message store and will not be available for review through the TUI.

The system resets the MWI to reflect the new message store.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. Do one of the following:
   - To locate an existing user, in the **Identifier** field, enter a possible identifier and click **Edit**.
   - To add a new user, in the Add a new user area, click **Add**.
3. Enter the appropriate information in the fields.
   For more information, see User Management Properties field descriptions on page 139.
4. Select a storage destination from the **Storage destination** drop-down list.
   If you select Microsoft Exchange as your storage destination to support the Exchange users, the system enables the **Automatic Mail Forwarding** field in the System Ports and Access Web page.
5. In the **Exchange email address** field, enter the email address of the Exchange user.
   The system displays this field only if you select **Microsoft Exchange** in the **Storage destination** field.
6. Click **Save**.
   The Messaging system validates the values you entered in the fields before saving the details.

Next steps

Administer the application role. See Initial administration checklist for application roles on page 58.

Chapter 5: Initial administration of the application role

Deployment scenarios

This chapter contains instructions to prepare each application role in your network topology for a specific site. Depending on the number of application roles in your network topology, you must complete some of the instructions more than once. Use the following scenarios and the checklist to help you plan your administration activities.

Each of the following deployment scenarios refers to the tasks in Initial administration checklist for application roles on page 58. For more information about your deployment options, see *Avaya Aura® Messaging Overview and Specification*.

One server and one site

In this scenario, associate one application role with a site by completing the first five tasks in the initial administration checklist. You can skip the remaining tasks.

Multiple servers and one site

In this scenario, you must associate more than one application role with one site. For example, your topology could be a site in Atlanta that has three dedicated application servers.

For this example, you would complete:

- Tasks 1 through 5 on the first application server
- Tasks 1, 3, and 6 on the second and third application servers

Multiple servers and multiple sites

In this scenario, you have at least two sites and you must associate one or more application roles to each site.

For example, if your topology is:

- A site in Atlanta with three dedicated application servers
- A site in Boston with one dedicated application server

In the first site, Atlanta, you would complete:

- Tasks 1 through 5 on the first application server
- Tasks 1, 3, and 6 on the second and third application servers

In the second site, Boston, you would complete tasks 1 through 5.

Important:

Do not restore system files that you backed up for one site on to application servers associated with a different site.

Initial administration checklist for application roles

Use the following checklist as a guide for setting up application roles for the first time. In large organizations with specialized administration roles, the Messaging administrator usually completes these tasks.

Because you must ensure that all application roles that support a specific site are identical, back up the first application server after you finish the administration tasks in this chapter. Use the restore procedure to load the backed-up data set on to subsequent application servers. Note that:

- You can restore data sets only to application servers that support the *same* site.
- You must integrate *each* application server with the telephony server individually. The backup routine does not capture the settings on the Telephony Integration Web page.

Perform the following tasks:

No.	SMI page	Task	On first application server of first site	On first application server of subsequent site	On subsequent server in any site
1	Telephony Integration	Integrating with the telephony server on page 60	Yes	Yes	Yes
2	System Parameters	(Optional) Enabling fax on page 66	Yes	Yes	No
3	Language Packs	Configuring languages on page 68	Yes	Yes	Yes
4	AxC Address	Changing the AxC IP address on page 70	Yes	Yes	No, if multi-server topology
5	Backup Now	Backing up application files on page 72	Yes	Yes	No
6	View/ Restore Data	Restoring application files on page 73	No	No	Yes

No.	SMI page	Task	On first application server of first site	On first application server of subsequent site	On subsequent server in any site
7	Validate Messaging configuration	Messaging configuration checklist on page 74	-	-	-

Telephony integration

Integration requirements

To establish a communications link between Messaging and your telephony server, you must ensure that certain parameters for each application role match the equivalent parameters on the telephony server.

Messaging supports the T.38 codec for receiving faxes. Ensure that the telephony server uses the T.38 fax codec for fax calls that route to Messaging.

Telephony parameters

Before you begin setting parameters on the Telephony Integration Web page, gather information about the following settings from the telephony server:

- Call Control Per Hop Behavior (PHB) and Audio PHB. This information is only relevant if your IP network infrastructure supports the Quality of Service (QoS) features.
- The transport method.
- The IP address and port number of each far-end connection, that is, the SIP proxy server.
- Domain name: The domain names must match for the application server, the telephony server, System Manager, and SIP Enablement Services.
- The number of messaging trunks.
- (Optional) The type of Secure Real-time Transport Protocol (SRTP) media encryption.

Network parameters

You also need the following information for each application server:

- The port number, usually 5060 for TCP transport or 5061 for TLS transport.
- The domain name.

Support for SIP INFO messages on SIP connections

Messaging supports out-of-band DTMF using the SIP-INFO method. When there is a mix of telephony vendors in the network, the lowest common denominator, that is, the system uses the SIP-INFO method for passing DTMFs for all telephony vendors to interwork properly.

Messaging accepts the INFO messages over SIP connections from Avaya Aura® Session Manager or AudioCodes gateway or any telephony server that supports SIP-INFO for DTMF. Messaging interprets the received INFO messages as if these messages had been received in the RTP stream using standard RFC 2833 DTMF signals. Session Manager, or AudioCodes gateway, or telephony server then routes the SIP-INFO messages along with the rest of the SIP signaling messages to the dialog to which the SIP-INFO messages belong.

There are two INFO formats, and both are accepted by the Messaging system to ensure maximum possible interoperability.

Format Number 1: This is the most popular format. This is an example of the DTMF digit 5 with a duration of 160 milliseconds:

```
INFO sip:7007471000@example.com SIP/2.0
Via: SIP/2.0/UDP alice.uk.example.com:5060
From: <sip:7007471234@alice.uk.example.com>;tag=d3f423d
To: <sip:7007471000@example.com>;tag=8942
Call-ID: 312352@myphone
CSeq: 5 INFO
Content-Length: 24
Content-Type: application/dtmf-relay
Signal=5
Duration=160
```

Format Number 2: This is an example of the DTMF digit 5:

```
INFO sip:7007471000@example.com SIP/2.0
Via: SIP/2.0/UDP alice.uk.example.com:5060
From: <sip:7007471234@alice.uk.example.com>;tag=d3f423d
To: <sip:7007471000@example.com>;tag=8942
Call-ID: 312352@myphone
CSeq: 5 INFO
Content-Length: 1
Content-Type: application/dtmf
5
```

Integrating with the telephony server

If your site includes more than one application server, you must complete these instructions on each application server in your site.

Before you begin

- Complete all the tasks in Initial administration checklist for the storage role on page 37.
- Gather information about the parameters from the telephony server that are required for integration. See Integration requirements on page 59.

Procedure

1. On the **Administration** menu, click **Messaging** > **Telephony Settings (Application)** > **Telephony Integration**.
2. Enter the appropriate information in the fields.

   For more information, see Telephony Integration field descriptions on page 61.
3. Click **Save**.
4. Restart Messaging.

   For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

   To validate the Messaging telephony integration, see Telephony Integration Checklist on page 65.

Next steps

- If you are administering the first or the only application role for a site, see Enabling fax on page 66.
- If you have completed all of the administration and backup tasks for the first application role in a multiserver topology, and you want to administer another application role, see Restoring application files on page 73.

Telephony Integration field descriptions

Name	Description
BASIC CONFIGURATION	
Switch Integration Type	Messaging uses SIP integration. The SIP SPECIFIC CONFIGURATION section is available only for SIP integration.
IP Address Version	The version of the IP address.

Name	Description
SIP SPECIFIC CONFIGURATION	
Transport Method	The telephony server uses the transport method for SIP signaling. The transport method of the application server and the telephony server must match. The types of transport methods: • TCP: Not encrypted. Use port 5060. • TLS: Encrypted. Use port 5061.

Name	Description
Far-end Connections	The total number of SIP proxy servers. The valid far-end connections: • Direct (no proxy): Select 1. • Session Manager: Select a maximum of 12. • SIP Enablement Services: Select 1. • AudioCodes gateway: Select a maximum of 4. • Other application servers for the same site. The number of **Connection** fields expand to match the number you select.
Connection x	The IP address and the port number of each far-end connection. If you select more than one far-end connection, the system accepts incoming calls from any of the servers on the connection list. The system attempts to place outgoing calls to the first server that accepts a connection in the order that you listed. MWI only uses one connection regardless of the number of sites or servers in your deployment.
Messaging Address	The IP address of the near-end application server. This address is always a read-only field. The port numbers: • TCP = 5060 • TLS = 5061
SIP Domain	The domain names of the application server and the far-end connection, which must match. Example: sip.example.com
Messaging Ports	The maximum number of active calls to or from a user. The range of the Call Answer Ports is 2 to 100.
Switch Trunks	The number of trunk members for Messaging on the telephony server. • The minimum is the number of call answer ports plus one. • The maximum is 120 trunk members on the telephony server. Trunk members in excess of the call answer ports are for features such as transfer, which require additional switch trunks. The number in the **Switch Trunks** field must match the number of trunk members on the telephony server if that server specifies a maximum.

Name	Description
Advanced Options: When the Advanced Options area is hidden, the system displays the **Show Advanced Options** button. If you click **Show Advanced Options**, the button changes to **Hide Advanced Options** and the system displays the following fields.	
Quality Of Service	Use this field if your IP network infrastructure supports the QoS feature. Accept the default values in QoS or enter new values. The values must match the number in the network region of the telephony server that the Messaging-signaling group uses. The range for both fields is 0 to 63. • Call Control PHB sets the quality of service level for call control messages. • Audio PHB sets the quality for audio streams.
UDP Port Range	The range of port numbers used by User Datagram Protocol (UDP) for Real Time Protocol (RTP). The default range is 8000 through 10000. • You can change the **Start** value. • The system uses the number of available trunks to calculate the **End** value. Ensure that the range of ports that you allocate to UDP does not conflict with ports used for other purposes.
Media Encryption	The type of Secure Real-time Transport Protocol (SRTP) media encryptions that the telephony server uses. This field is optional.
SIP INFO for DTMF	The SIP INFO messages for DTMF out-of-band. Select one of the following options: • **Ignore**: To ignore all SIP INFO DTMF digits in the signaling stream. • **Accept**: To accept all incoming SIP INFO messages for the two formats and interpret the messages received in the RTP stream as RFC 2833-compliant digits. The system sends outbound DTMF as SIP INFO messages with application type dtmf-relay with a specified duration of 250 ms. The default value is **Ignore**. For more information on SIP INFO message formats, see Support for SIP INFO messages on SIP connections on page 60.
Media Encryption During CapNeg	When capability negotiation (CapNeg) is present in Session Description Protocol (SDP), Media encryption is required.

Name	Description
	The options are: • **Enabled**: To activate the default value. • **Disabled**: To change the value in the **Media Encryption** field to **None**. Messaging automatically changes the value, and you cannot change the value. Select **Disabled** only if required for a specific telephony integration. For more information, see the configuration notes.
Supported Header includes “replaces”	The supported header must include the replaces value so that endpoints reflect their capabilities in the SIP headers and Messaging communicates effectively with a specific telephony integration. The options are: • **no**: The default value. • **yes**: Only for a specific telephony integration. For more information, see the configuration notes.
Monitor Far-end OPTIONS messages	Messaging proactively monitors the SIP OPTIONS messages that the far-end sends. If Messaging does not receive a SIP OPTIONS message from the far-end within the time specified in the **Proactive Interval** field, then Messaging considers the far-end as nonfunctional or unreachable. The options are: • **no**: The default value. • **yes**: Set the value in the **Proactive Interval** field to the interval for which the far-end is configured for sending the OPTIONS message. The value must be in seconds.
Inactive Link Actions	Only available if the value in the **Monitor Far-end OPTIONS messages** field is set to yes. The options are: • **Alarm Only**: Messaging generates an alarm whenever an expected OPTIONS message does not arrive within the **Proactive Interval** period plus 30% of that time. On the next receipt of SIP OPTIONS or the next incoming call, the system clears the alarm. • **Close Connections**: Messaging generates an alarm, closes all incoming connections, and drops all active calls at that point.
SIP REFER Delay	The delay of the transfer operation in milliseconds when a Messaging outbound call is answered and the SIP REFER request sent. The value range is between 0 to 5000 milliseconds.

Name	Description
Enable Basic Transfer	The option to enable and disable the Basic Transfer feature. If you select this check box, Messaging performs a blind transfer operation and does not directly call the destination endpoint. The gateway of the Messaging network establishes the call and transfers the two endpoints. Because the gateway establishes the call, the caller ID might change. **Note:** If you enable the Basic Transfer feature, Messaging does not support SIP UUI.

Telephony Integration Checklist

Use this topic to validate the Messaging telephony integration.

Before you begin

The Pilot number needs to be configured on the telephony server.

Check	Steps	Result / Validate
Inbound calling	Call an extension and ensure that the system routes the call to the application role server.	When a call covers to voice mail, you must hear ringing and then the system main menu. This validates the call coverage functionality.
Outbound calling	Make an outbound call through the **Call-out** diagnostics test. In the **Select the test(s) to run** drop-down list, select **Call-out**. For more information about the Call-out test, see *Running application server diagnostics*.	Test a call to an: • extension: Verify that the system connects the call to the extension. • outside number. Verify that the system connects the call to the outside number. Ensure to keep the call up for 60 seconds. This validates outbound calling to internal and external numbers.
MWI	Verify the MWI function through the **MWI** diagnostics test. In the **Select the test(s) to run** drop-down list, select **MWI**.	Observe that the MWI goes on, off, and then on. This validates the MWI.

Check	Steps	Result / Validate
	For more information about the MWI test, see *Running application server diagnostics*.	

Implementing fax

Using Messaging, you can receive incoming faxes through the inbound (native) fax and third-party methods. In order to provide fax capabilities to users in Messaging, you must perform the following:

1. Ensure that the telephony server uses the T.38 fax codec for fax calls.
2. Administer the external SMTP host. For more information, see Administering the external SMTP host on page 41.
3. Configure the CoS for fax support. For more information, see Class of Service field descriptions on page 158.
4. Configure the application server to receive fax. For more information, see Enabling fax on page 66.
5. In User Preferences, specify the email address where you want the system to forward the fax.

For information on configuring Messaging to transfer fax calls to a fax server, see System Parameters field descriptions on page 125.

Related topics:

Enabling fax on page 66

Enabling fax

Important:

If your deployment includes more than one server in the application role, only enable fax for the first server in the site. You can administer the servers for subsequent application roles by backing up the first application role and then restoring the data on to the server for the subsequent application role. See Initial administration checklist for application roles on page 58 for information about which procedures are to be done manually on the server and which are done automatically through the backup and restore process.

Before you begin

- If you are administering the first or the only application role, you must first complete the procedure for Integrating with the telephony server on page 60.
- Your IT network must include a fax server.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **System Parameters**.
2. Enter the appropriate information in the **Fax** area.
   See System Parameters field descriptions on page 125.
3. Click **Apply**.
   The system displays a confirmation message.
4. Click **OK** to proceed.

Next steps

- If you are administering the first or the only application role for a site, see Configuring languages on page 68.
- If you are administering additional application servers that support the *same* site as the first server, see Restoring application files on page 73.

Language packs

You must always install language packs on servers with the application role. Language packs are site specific, that is, the list of language packs that the Messaging system displays in User Preferences for a user is dependent on the language packs installed on the application server serving that site.

If there is a cluster of application servers for a specific site, then the Messaging system retrieves the list of language packs that you installed from the first application server. Hence, you need to ensure that you install the same set of language packs on all cluster members.

Messaging supports users who are hearing impaired or speech impaired. Such users can transmit and receive text using a teletypewriter (TTY) device. You must install the *English (United States) - TTY* language pack to use the TTY functionality.

Configuring languages

Note:

If you have upgraded the Messaging system, you must perform this task to reinstall the language packs that you installed prior to the upgrade. You must have recorded these language pack names during the upgrade process as specified in the *Upgrading Avaya Aura® Messaging* document.

You must install language packs and select the languages for your site on the Languages Web page. The following system features use the languages that you select on this page:

- User Preferences
- The telephony user interface (TUI)
- Name playback
- TTY

Important:

If your deployment includes more than one server in the application role, you must configure languages on every application server. See Initial administration checklist for application roles on page 58 for information about which procedures are to be done manually on the server and which are done automatically through the backup and restore process.

Before you begin

If you are administering the first or the only application role, you must first complete the Enabling fax on page 66 procedure.

About this task

You must install the standard prompts language pack. Rapid prompts language pack is optional and is currently only available in US English for Aria TUI. Standard prompts provide more detailed information than rapid prompts. Rapid prompts help the user save time because these prompts are much shorter. Hence, rapid prompts are for users familiar with the TUI capabilities.

If you setup rapid prompts on your system, the end user can view the rapid prompts check box on the My Phone Web page in User Preferences.

Messaging offers the Audix® TUI, which provides support for TTY users.

Important:

You cannot uninstall a language pack. However, if you need support with language packs, contact Avaya Services.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **Languages**.
2. In the **Add Language Pack** field, click **Choose File** and navigate to the location of the language packs that you want to add to this application server.
3. Click **Open**.
4. Click **Upload**.

   For more information, see Languages field descriptions on page 69.

   Note:

   When you add a language pack, the system drops all active calls. Additionally, the Messaging system will be unavailable for some time.
5. Click **Apply**.
   The system saves the language packs that you added.
6. After you install all the language packs, reload the user list and the global address list.

   For more information, see Loading lists on page 175.

Next steps

- If you are administering the first or the only application role for a site, see Changing the AxC IP address on page 70.
- If you are administering additional application servers that support the *same* site as the first server, see Restoring application files on page 73.

Languages field descriptions

Name	Description
Language Packs: Installed Languages	
Name	The list of language packs that you installed.
User Selectable	The language for User Preferences and TUI. If you install multiple languages, users can select their preferred language.
Language Settings	

Name	Description
System Language	The system uses the value in this field as a backup language setting in case the application server cannot obtain the site configuration from the storage server. The system uses the site language configuration to determine the language that the caller or the user hears.
Default Subscriber UI Language	The language of the user interface. The system uses the value in this field as a backup language setting in case the application server cannot obtain the site configuration from the storage server. If you install multiple languages, users can select their preferred language.
Language Packs	
Current Application software release	The version number of the Messaging system.
Add Language Pack	Navigate to the location of the language packs that you want to add to this application server.

Changing the AxC IP address

Avaya ships Messaging servers that are set up for a single-server topology. Skip this procedure if you have a single-server topology.

The AxC connects the storage and the application roles. In a single-server topology, these roles are on the same server, and you can use the default settings. However, if you have a topology with more than one server, you must change the default AxC IP address on *each* dedicated application server.

Use the AxC Address Web page to secure Web services communication between an application server and the associated storage server. However, if this is a single server, that is, the application and storage roles are defined on the same server, then you do not need to make the connection secure as all Web services communication is internal to the server.

Important:

If your deployment includes more than one server in the application role, only change the AxC IP address for the first server in the site. You can administer the servers for subsequent application roles by backing up the first application role and then restoring the data on to the server for the subsequent application role. See Initial administration checklist for application

roles on page 58 for information about which procedures are to be done manually on the server and which are done automatically through the backup and restore process.

Before you begin

- Administer the storage role. See Initial administration checklist for the storage role on page 37.
- If you are administering the first or the only application role, you must first complete the procedure for Configuring languages on page 68.
- On the AxC server, the server has been added in the Messaging system topology as an application server. For more information, see Adding the first application server on page 96.

Procedure

1. On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **AxC Address**.
2. In the **AxC IP address** field, enter the IP address of the storage server.

   By default, the Messaging system populates this field with the IP address of the local host. Ensure that the AxC address is the IP address of the operational AxC server.
3. To secure the communication of Web services with the AxC, click **https://**.
4. Click **Apply**.
   The system displays a confirmation message.
5. Click **OK** to proceed.

Next steps

- If you want to validate your Messaging configuration, see Messaging configuration checklist on page 74.
- If there is only one application server on your site, you are ready to define your site and topology. For more information, see Initial administration checklist for sites and topology on page 81.
- If there are several application servers on your site, you must configure each server so that all the servers are identical in the cluster. To make all the servers identical, back up the application server you configure and restore the data on each application server. For more information, see:
  - Backing up application files on page 72
  - Restoring application files on page 73

Backing up application files

When your Messaging topology includes more than one application role for a specific site, you must configure all application roles that support the site identically. To ensure this, back up the first server you configure and then copy the server files to subsequent application servers.

If your topology includes multiple sites, the sites will have different settings. For example, different dial plans. Therefore, do not restore backed-up files from one site to servers that support a different site.

The time taken for backup will vary depending on the amount of data.

Before you begin

Before backing up the application role, ensure that:

- You obtain login credentials to a FTP server for storing the application backup data.
- You have completed all administration tasks for the first or only application role. See Initial administration checklist for application roles on page 58.
- Messaging is not running.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **Backup Now**.
   The system displays the Backup Now Web page.
2. In the **Data Sets** area, select **Specify Data Sets**.
3. Select the **Messaging** check box, and then select **Messaging Application**.
4. In the **Backup Method** area, select **Network Device** and then choose a location for the backed-up files by completing the following fields:
   - **Method**: Select one of the following methods from Secure Copy Protocol (SCP), File Transfer Protocol (FTP), and Secure File Transfer Protocol (SFTP).
   - **User Name**
   - **Password**
   - **Host Name**: Enter the host name or IP address.
   - **Directory**: Enter the full directory path where your backup will be stored.

   For more information, see Backup Now field descriptions on page 214.

   You will need this information when you restore the data set to other servers.
5. Click **Start Backup**.

The system starts the data backup.

Next steps

Restore the backed-up data set on to all additional application servers for the site. See Restoring application files on page 73.

Restoring application files

If your Messaging topology includes more than one application role for a specific site, restore the Messaging application data set that you previously backed up on to each subsequent application server for the site.

If your topology includes multiple sites, the sites will have different data sets. Therefore, do not restore backed-up files from one site to servers that support a different site. Instead, repeat the procedures in this chapter on a per-site basis.

Before you begin

Before restoring previously backed-up data sets:

- Integrate the application server for a site with your telephony server.
- Ensure that you have the information that you entered on the Backup Now Web page.
- Ensure that Messaging is not running.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **View/Restore Data**.
2. In the **View current backup contents in** area, select **Network Device** or **Local Directory**. Use the same information that you used when you backed up the data:
   a. **Method**
   b. **User Name**
   c. **Password**
   d. **Host Name**
   e. **Directory**
3. Click **View** and then select the **audix-ap** backup file.
4. Click **Restore**.

   If there is a mismatch between the server names or backup versions, you must perform a force restore.

   Repeat these steps for each additional application server.
5. Restart Messaging.

For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Next steps

- If you have additional application roles to administer on your site, repeat these instructions on each additional application server. When you finish, administer your site and topology. See Initial administration checklist for sites and topology on page 81.
- If you want to validate your Messaging configuration, see Messaging configuration checklist on page 74.

Messaging configuration checklist

This topic outlines a procedure for validating the Messaging configuration.

Prerequisites:

- You have completed the installation and configuration of the Messaging system.
- You have installed the Microsoft Outlook form using Microsoft Exchange.
- You have configured the Microsoft Outlook client for each test user for IMAP access.

Tasks	Steps	Result / Validate
Check whether all the services are running	Verify the status of the: • storage role. For more information, see Verifying the status of the storage role on page 40. • application role. For more information, see Verifying the status of the application role on page 348.	All required services are up and running.
Create test users	Add the following test users: • Create Test User1 with the *Standard* CoS setting. • Create Test User2 with the *Enhanced* CoS setting. For more information, see Adding users on page 134.	To check whether the system creates the test users, click **Messaging** > **Reports (Storage)** > **Users**.

Comments? infodev@avaya.com

Tasks	Steps	Result / Validate
Configure test users	Open User Preferences for Test User1 and set the following: • Select the General page and enter a valid mobile number in the *Mobile Phone or Pager* area. • Select the Notify Me page and enable text Notifications using the *With a text message or page to:* option using the number you configured in the General page. • Select the Notify Me page and enable Email Notifications by providing a valid email address. Messaging supports only email based (SMTP) pager and cellular notifications. For more information, see Changing user properties on page 136 and the *Using Avaya Aura® Messaging* guide.	
	Open User Preferences for Test User2 and set the following: • Select the General page and enter a valid mobile number in the *Mobile Phone or Pager* area. • Select the Notify Me page and enable Phone Notifications using the number you configured in the General page. • Select the Reach Me page and enable and configure two Reach Me numbers that consist of an internal extension and an external number.	

Tasks	Steps	Result / Validate
	Messaging supports only email based (SMTP) pager and cellular notifications. For more information, see Changing user properties on page 136 and the *Using Avaya Aura® Messaging* guide.	
User initialization	As Test User1, perform the following: • Call the Pilot Main Number from a phone registered to the extension assigned to the user. Ensure that this call is up for at least 60 seconds. • Provide temporary password as per system prompts. • Change password. • Record spoken name. • Record greeting. • Hangup. For more information, see the *Using Avaya Aura® Messaging* guide.	If you are calling: • from an extension registered to the test user, the system prompts you to enter the temporary password. Upon entering the temporary password, the system guides you through the steps to initialize your mailbox. • from a number that is different from the one registered to any other user, you hear the Main Menu prompt. Upon entering your Mailbox and Password, the system guides you through the steps to initialize your mailbox. This validates: • Users are loaded appropriately on the Messaging server. • Integrated login. • Long duration outbound calls through any SBCs or gateways.
	As Test User2, perform the following: • Call the Pilot Main Number from a phone that is not registered to the extension assigned to the user. • Press # to login as per system prompts and provide the mailbox number. • Provide temporary password as per system prompts. • Change password. • Record spoken name.	

Tasks	Steps	Result / Validate
	• Record greeting. • Hangup. For more information, see the *Using Avaya Aura® Messaging* guide.	
Basic call answer	Perform the following: • From extension of Test User2, call direct extension number for Test User1 and let the call roll over to voice mail. • Leave a message; note user details, and date and time when the message is sent. • Hangup. • From an outside number, dial external Pilot number and enter Test User1 extension. • Leave a message; note outside number, and date and time when the message is sent. • Hangup. For more information, see the *Using Avaya Aura® Messaging* guide.	Observe the following: • No Answer greeting for Test User1 plays in first case and busy greeting plays in second case. • The system plays greeting for User1. • MWI changes for Test User1 to On. • Email notification delivery, text message notification delivery, and subject line - Voice Message from Test User2 (ext#here)) for first two calls. - Voice Message from (external#here) for third call. This validates: • Basic Call Answering • Basic MWI functionality • Email notifications • Text message notifications • Subject line matching
Basic messaging	Perform the following: • From extension of Test User1, call main pilot number. • Provide password to login as per system prompts. • Listen to both messages - do not delete. • Observe MWI turns Off.	Observe the following: • Test User1 has two messages in inbox with appropriate time. • MWI updates to Off for Test User1.

Tasks	Steps	Result / Validate
	For more information, see the *Using Avaya Aura® Messaging* guide.	This validates: • Ability to retrieve messages via TUI. • MWI updates. • Subject line matching.
Outcall notification. You might skip these steps, if you do not plan to use this feature.	Perform the following: • Configure Enhanced CoS to allow Outcalling notification. Select the *Enhanced* CoS from the **Class of Service** drop-down list. Set **Allow outcalling notification** to *Yes*. In order to shorten test time, change the **Start after** value for outcalling notification to be *5* minutes. • From extension of Test User1, call main pilot number. • Provide password to login as per system prompts. • Create a voice message for Test User2; note user details, and date and time message is sent. • Address the outcall for future delivery in n minutes. • Verify that outcall is launched after n+5 minutes. Ensure that this call is up for at least 60 seconds. • Reset the **Start after** value to real system value. For more information, see Changing a Class of Service on page 156 and the *Using Avaya Aura® Messaging* guide.	Observe the following: • The system does not deliver the message until expected date and time. • Date and time stamp of message is as per expected future delivery date. • Outcall notification occurs as per schedule setting and only after the system delivers the message. This validates: • System date and time is correct. • Outcall Notification. • Long duration outbound calls through any SBCs or gateways.

Tasks	Steps	Result / Validate
Using Outlook toolbar. You might skip these steps, if you do not plan to use this feature.	Perform the following: • As Test User1, set up the IMAP account. • As Test User1, log in to the IMAP account using Outlook and inspect voice messages. • Use Play on PC for a message. • Use Play on Phone for a message. • Test Help link on Outlook Toolbar. • Select User Preferences Link on Outlook toolbar and login. For more information, see the *Using Avaya Aura® Messaging* guide.	Observe the following: • The system plays the message using the media player for playing on PC. • The system plays the message using the TUI for playing on phone. • All messages have correct date and time, and subject line information. • Online Help for toolbar is accessible. • User Preferences is accessible. This validates: • Most Outlook form actions. • Subject line matching. • Access to online help. • DNS for User Preferences is correctly set.
Reach Me. You might skip these steps, if you do not plan to use this feature.	Perform the following: • Call the extension for Test User2. • Do not answer any call. For more information, see the *Using Avaya Aura® Messaging* guide.	Observe the following: • The system notifies the caller that Test User2 is not answering and that other numbers are being tried. • The system calls each configured number in the set order. • After failing to get an answer for both numbers, the system allows the caller to leave a voice message. This validates the Basic Reach Me functionality for both types of phone numbers.

Tasks	Steps	Result / Validate
AA call transfer to user. You might skip these steps, if you do not plan to use this feature.	Perform the following: • Call Auto Attendant number. • Enter Test User1 Extension. • Answer Call. • Call Auto Attendant number. • Enter Test User2 extension. • Do not answer call and allow Reach Me. • Answer second Reach Me number. For more information, see the *Using Avaya Aura® Messaging* guide.	Observe the following: • Call reaches Test User1 extension and talk path is correct. • Call reaches Test User2 extension, system invokes Reach Me, and talk path is correct. This validates: • Users are loaded appropriately on the application server. • Basic Auto Attendant functionality. • Speech addressing, if enabled. • Reach Me using Auto Attendant.

Chapter 6: Sites and topology

Initial administration checklist for sites and topology

Use the following checklist as a guide for administering the sites and topology of Messaging for the first time. In large organizations with specialized administration roles, the Messaging administrator usually completes these tasks.

Complete the tasks in the following sequence:

			Location		
No.	**SMI page**	**Task**	**Single-server systems**	**Front-end / Back-end systems**	✔
1	Sites	Setting site properties for the first time on page 83	Single server	Storage server	
2	Sites	Defining dial rules on page 85	Single server	Storage server	
3	Sites	Assigning an attendant number on page 86	Single server	Single server	
4	Sites	Adding sites on application servers on page 87	Single server	Storage server	
5	Sites	Assigning language menu choices for a site on page 88	Single server	Storage server	
6	Topology	Adding the first application server on page 96	Single server	Storage server	
7	Topology	Adding additional application servers on page 97	—	Storage server	
8	Cluster	Configuring a cluster on page 99	—	Each application server in the cluster	
9	System Operations	Verifying the link to the AxC on page 103	Single server	Each application server in the cluster	

Initial site administration

Overview for administering sites

Site-specific properties are stored on the storage server, which automatically applies these properties to each application server associated with any given site.

You can set site-specific properties on the Sites Web page in the SMI. When setting up a new site, you must enter data in the fields in the **Main Properties** area. You can complete the other fields on this page later.

After you define the site by entering the main properties, the storage server and all the associated application servers become a Messaging system.

You can use the Sites Web page to configure the following common settings for a group of users:

- Inbound and outbound dial rules.
- Default prompt language when a user calls into Messaging. The user has an option to select from multiple languages using menu choices, if configured.
- Speech recognition language.
- Language prompts presented by the system when callers leave messages for the mailbox of a user within the site. This includes TTY and multilingual prompts.

The Sites Web page includes important configuration information that the application server depends on. The system generates an alarm if an error occurs while fetching the data from AIC or when writing to ADCS.

When the system generates the alarm, the TUI uses the Sites Web page data from the cache, which might not necessarily be the same as that in the AIC.

The system resets the alarm every time the application server downloads or refreshes the data from the Sites Web page. The Sites Web page data is downloaded or refreshed:

- During the nightly synchronization of cache data.
- By clicking **Application Distribution Cache (ADCS)** on the System Operations Web page.

Improved multisite support including full E.164 Dial Plan support

Messaging provides the ability to centralize the system using full E.164 mailbox numbers, yet each site has the ability to have short mailbox numbers.

You can configure mailbox numbers using less than the full E.164 number and map these mailbox numbers to a full E.164 number. Thus, users at any site can continue to use mailbox

numbers locally that are smaller in length, but are still uniquely identifiable in the global context.

Messaging supports only those mailbox numbers that have a fixed length system-wide. Messaging does not support those mailbox numbers that have a variable length.

Setting site properties for the first time

If you are the administrator who sets site properties for the first time, you must ensure that Messaging works properly. You might have to decide whether to enable Auto Attendant and to set up the system greeting. You can set these properties later, but you must set the Main Properties first.

About this task

Your Messaging system includes a site named Default. You must change the name of this site and enter information about the primary messaging mailbox of your organization.

Complete the following instructions on the storage server.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Sites**.
2. Complete the fields in the **Main Properties** area.
   For more information, see Sites field descriptions on page 89.
3. (Optional) If your organization has decided to enable Auto Attendant, complete the fields in the **Auto Attendant** area. You can complete this step later.
4. (Optional) If your organization has provided you with .wav files for a system greeting or a speech recognition message, complete the fields in the **Auto Attendant Greeting / Menu** area. You can complete this step later.
5. Click **Save**.
   The system displays the name of your site in the **Site** drop-down list.
6. Restart Messaging.
   For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Next steps

- To configure dial rules, see Defining dial rules on page 85.
- To add additional sites to your network, see Adding sites on application servers on page 87.
- If you do not want to add another site, see Overview for administering topology on page 95.

Dial rules

Migrating dial plan data from Messaging R6.0.1 SP3 or R6.1 to R6.2

If you upgrade Messaging from R6.0.1 SP3 or R6.1 to R6.2, you must manually move the data from the Dial Rules Web page, the Dial-Out Rules Script, and/or the Attendant/Operator Web page to the Sites Web page.

You must perform the following:

- Prior to the upgrade, note down the configuration in one of the application role server within a site or cluster.
- After the upgrade, enter the configuration data in the Sites Web page for the corresponding site.
- Return to the application role server Dial Rules Web page. In the **Dial plan handling style** field, select *Site definition based* and verify the upgrade by clicking **Test**.

The following table includes information on the fields that you must use after the upgrade.

Dial Rules Web page (Before upgrade)	Sites Web page (Post upgrade)	Comments
Country code	Country code	The country code of the dialing phone number.
Area code / Private number	National destination code	The beginning sequence of digits that the telephony server considers local other than the one defined for the telephony server.
Long-distance prefix	National prefix	The preceding digits before the area code of the dialing phone number.
International prefix	International prefix	The preceding digits before the country code of the dialing phone number.
Outside line prefix	Outside line prefix	The digits required to gain outside line access.
Number of digits in an extension	Subscriber number length (within this site's national destination code) Or Short extension length	If you are configuring an: • External (Public Network) Dial Plan Site, configure the length of digits required to call a number within the originating area code or a local call in the **Subscriber**

Comments? infodev@avaya.com

Dial Rules Web page (Before upgrade)	Sites Web page (Post upgrade)	Comments
		number length (within this site's national destination code) field. • Internal Dial Plan Site, configure the length of extensions for users on this site in the **Short extension length** field.
Number of DID ranges		This field has been deprecated.
Caller ID Internal Number Prefix		This field has been deprecated.
Dial-out rules		Use the fields in the Toll-Free and Premium Calls and Local Calls areas to configure the dial-out rules.

Attendant / Operator Web page (Before upgrade)	Sites Web page (Post upgrade)	Comments
Schedule type	Availability	Indicates whether the attendant is available.
Attendant (operator) extension	Operator (live attendant) extension	The extension number of the attendant.
General delivery mailbox number	General mailbox	The general mailbox for call answering in case the attendant is unavailable.

Defining dial rules

You can use dial rules for the following features:

- Reach Me
- Notify Me
- Play on Phone
- Personal Attendant

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Sites**.

2. Enter the appropriate information in the following areas:
   - **Site External (Public Network) Dial Plan**
   - **Site Internal Dial Plan**
   - **Toll-Free and Premium Calls**
   - **Local Calls**

   For more information, see Sites field descriptions on page 89.
3. Click **Save**.
4. Restart Messaging.

   For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Next steps

- To configure the attendant for a site, see Assigning an attendant number on page 86.

Assigning an attendant number

When a caller presses 0 to reach an attendant, the system transfers the call to the assigned extension. If the attendant does not answer, then the system transfers the call to a general-delivery mailbox so that the caller can leave a message.

The system preserves the language selection from the caller at the Auto Attendant menu when the system changes the call into a covered call, that is, Ring-No-Answer scenario. The system preserves the information for the following reasons:

- The system covers the call at another application server where you have not installed the corresponding language pack.
- You have not installed Communication Manager 6.2.

From the user point of view, the system presents the language menu to the caller at Auto Attendant. Additionally, if you configure the call-answering menu for the pilot number, the system presents another language menu to the user. You must configure only a single Auto Attendant pilot number per site. The Auto Attendant pilot number has the ability to support up to three languages.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Sites**.
2. In the Operator (Live Attendant) area, in the **Availability** drop-down list, select one of the following:

- Never (the default)
- Always

3. In the **Operator (live attendant) extension** field, enter the extension of the attendant.

   If you do not enter an extension number, when the caller presses 0, the Messaging system updates the caller that no operator is available and disconnects the call.

4. In the **General mailbox** field, enter the extension for a shared mailbox that is accessible to all attendants.

   If you enter an extension number in the **Operator (live attendant) extension** field and if the attendant does not answer the call, then the system transfers the call to this mailbox.

5. In the **Auto Attendant** area, click **Enabled**.
6. In the **Pilot Number** field, enter the pilot number for Auto Attendant.

   You must configure only a single Auto Attendant pilot number per site.

7. In the **Default Language** field, click the language that you want as the default for the Auto Attendant number.
8. You can select two additional languages for the Auto Attendant number.
9. Click **Save**.
10. Restart Messaging.

    For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Next steps

If you want to add additional sites to your network, see Adding additional sites on page 87.

Adding sites on application servers

Messaging supports up to three sites, one on each of the three application servers in the cluster.

About this task

Depending on your deployment requirements, you must add a site for each application server. Complete the following instructions on the storage server.

You must restart Messaging after you add a site.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Sites**.

2. On the Sites Web page, click **Add New**.
3. Enter the appropriate information in the fields.
   For more information, see Sites field descriptions on page 89.
4. Click **Save**.
5. Restart Messaging.
   For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Next steps

Define your system topology. See Overview for administering topology on page 95.

Assigning language menu choices for a site

You install language packs on application servers, and you create sites on a storage server. Hence, to create language menu choices for a site, you must follow the steps documented in the following task.

Before you begin

If you upgrade Messaging to Release 6.2, at a minimum you must reinstall those language packs that the Sites Web page used previously. For information on installing languages , see Configuring languages on page 68.

Procedure

1. Define a new site using the Sites Web page.
   For more information, see Setting site properties for the first time on page 83.
   The default language that the Messaging system associates with each site is US English, which is the default system language. No other language menu choice is available until you create a site-application server mapping.
2. Create the site-application server mapping using the Topology Web page.
   For more information, see Adding additional application servers on page 97.
3. To select from the available languages that you installed on the mapped application server, update the site that you created in Step 1 using the Sites Web page.
4. If you install a new language pack on the application server and want to update the existing site language menu with the new language pack, use the Sites Web page to select the language pack.
5. If you change the default site language, reload the user list and the global address list.

For more information, see Loading lists on page 175.

Sites field descriptions

Name	Description
Site	The list displays all your Messaging sites. You can add a new site or delete an existing site by clicking the appropriate button.
Main Properties	
Name	The name of the site. Messaging includes a site named Default. Change this name when you set the site properties for the first time.
ID	The ID of the site.
Internal Messaging access number	The internal number is the number the Messaging system expects to receive from the telephony server augmented with various prefixes. The internal telephone number is also known as the internal pilot number. In Messaging R6.1 and R6.2, Messaging analyzes the *SIP To:* header and checks the internal numbers of the configured site on all sites. After the system finds a matching site, Messaging processes the call using the selected site and the associated mailboxes.
External Messaging access number	The external number is the number the Messaging system uses in notifications and in the General Web page in User Preferences to inform the user how to reach the Messaging system from outside. A call to the external number results in identical call data when the call reaches the Messaging system, as a call to the internal number. The external telephone number is also known as the external pilot number.
Site Default Language	The list displays the languages installed on the application server or servers associated with a site. Use this option to select the default or the first language for a site. The default is the base language, which is US English. The system uses the language you select in this field to determine the language prompt that Messaging plays to callers leaving messages for all mailboxes within the site.
Additional Language	The list displays the languages installed on the application server or servers associated with a site. Use this option to select the additional language for a site. When you select an additional language, callers leaving messages for all mailboxes on this site receive a multilingual prompt.
Additional Language	The list displays the languages installed on the application server or servers associated with a site. Use this option to select the additional language for a site.

Name	Description
	When you select an additional language, callers leaving messages for all mailboxes on this site receive a multilingual prompt.
Site External (Public Network) Dial Plan: *Describe the public telephony network dial plan applicable to this site.*	
Country code	The country code of the dialing phone number.
International prefix	The digits preceding the country code of the dialed telephone number.
National prefix	The digits preceding the area code of the dialing phone number.
International dialing (to this country)	The option to prepend the national prefix code while making international calls. The options are: • **Do not prepend National Prefix**. • **Prepend National Prefix**.
National destination code	The beginning sequence of digits that the telephony server considers local other than the one defined for the telephony server.
Dialing within national destination	The option that the Messaging system uses for dialing within national destination. The options are: • **Do not prepend National Prefix or National Destination code**. • **Prepend National Prefix**. • **Prepend National Prefix and National Destination code**.
Subscriber number length (within this site's national destination code)	The length of digits required to call a number within the originating area code or a local call.
Outside line prefix	The digits required to gain outside line access.
Site Internal Dial Plan: *Describe the internal dial plan applicable to this site.*	
Short extension length	The extension length for users on this site.
Short mailbox length	The mailbox number length for users on this site. When the AxC returns mailbox numbers in the User List and Global Address List to the application servers, the AxC examines the following: • Long mailbox number as stored in the LDAP attribute for the user. • Site prefix for that user.

Name	Description
	For example, for a 5-digit based site, if the long mailbox number is 14085671234, then the site prefix is 40856, the site country code 1, the site mailbox length 5, and the short mailbox number 71234.
Extension style for telephony integration	The extension style for telephony integration. The system uses this value to set MWI on or off. The options are: • **Short** • **E.164** • **E.164 without leading +** The default value is **Short**. When a user receives a new voice message, the MWI light turns on. When a user listens to all received voice messages, the MWI light turns off.
Site prefix	The digits that precede the extension in a phone number. When the AxC returns mailbox numbers in the User List and Global Address List to the application servers, the AxC examines the long mailbox number as stored in the LDAP attribute for the user, the site prefix for that user, and then returns the short mailbox number. For example, for a 5-digit based site, if the long mailbox number is 14085671234, then the site prefix is 40856, the site country code 1, the site mailbox length 5, and the short mailbox number 71234.
National mailbox number convention	The numbering convention for the national mailbox. The options are: • **Always prepend national prefix**. • **Never prepend with national prefix**. • **Optionally prepend national prefix**.
Universal addressing	The mailbox numbers that the system recognizes for users in this site: • **local** • **national** • **global**
Toll-Free and Premium Calls: Call classification information for outbound national calls, required to determine whether the call is allowed given the dial-out privilege in the associated user's Class of Service.	
Toll-free codes	The area codes of toll-free calls, which the users can dial. Enter national destination codes only. Do not include the national prefix. A semi-colon (;) separates the numbers.
Premium Number codes	The code used for dialing premium number calls. The code you enter in this field is a restricted code. If you do not have the necessary permissions, Messaging rejects the outbound national call.

Name	Description
	Enter national destination codes only. Do not include the national prefix. A semi-colon (;) separates the numbers.
Local Calls: Call classification information for outbound local calls, required to determine whether the call is allowed given the dial-out privilege in the associated user's Class of Service.	
This site contains users whose Class of Service dial-out privilege allows only local calls	Select this check box if the site includes users for whom the CoS dial-out privilege allows only local calls.
Not all local calls (calls within the national destination code's area) are charged as local calls	Select this check box if the system does not charge all the local calls as local calls. To enable this check box, select the **This site contains users whose Class of Service dial-out privilege allows only local calls** check box.
Subscriber number ranges considered local	The user number ranges that the system considers local. Define ranges using the initial left most digits only. Do not include the national destination code. Use semicolons to separate multiple ranges. To enable this check box, select the **Not all local calls (calls within the national destination code's area) are charged as local calls** check box.
Some national calls (calls outside the national destination code's area) are charged as local calls	Select this check box if the system charges some national calls, calls outside the area of the national destination code, as local calls. To enable this check box, select the **This site contains users whose Class of Service dial-out privilege allows only local calls** check box.
National number ranges considered local	The national number ranges that the system considers local. Define ranges using the initial left most digits only. Do not include the national prefix. Use semicolons to separate multiple ranges. To enable this check box, select the **Some national calls (calls outside the national destination code's area) are charged as local calls** check box.
Operator (Live Attendant)	

Name	Description
Availability	The options to indicate whether the attendant is available. The options are: • **Never** • **Always**
Operator (live attendant) extension	The extension of the attendant or live operator.
General mailbox	The general mailbox for call answering in case the attendant is unavailable.
Auto Attendant	
Auto Attendant	Use the option to enable or disable the Auto Attendant feature. The default is *disabled*. The system routes the Auto Attendant to the station, that is, the Auto Attendant transfers callers to local extensions.
Pilot Number	The pilot number for Auto Attendant. You must configure only a single Auto Attendant pilot number per site. Each Auto Attendant can support up to three languages. Each Auto Attendant pilot-number-language group setting represents an Auto Attendant language selection menu for that pilot number.
Default Language	The languages that you installed on the application server associated with a site. Use this option to select the language for the Auto Attendant number associated with a site. The Messaging system associates the selected Auto Attendant language with all users belonging to that site. The default language that is associated with each Auto Attendant is US English, which is the default system language.
Additional Language	The languages that you installed on the application server associated with a site. Use this option to select the additional language for the Auto Attendant number associated with a site. By selecting additional languages, users can select the language of their choice with one single multilanguage greeting. The user can choose from a maximum of three languages.
Additional Language	The languages that you installed on the application server associated with a site. Use this option to select the additional language for the Auto Attendant number associated with a site. By selecting additional languages, users can select the language of their choice with one single multilanguage greeting. The user can choose from a maximum of three languages.
Additional sites included in the directory	The name of another site *with the same dialing plan* in a multisite deployment.

Name	Description
	Each site has its own Auto Attendant directory. By default, all users who are associated with a given site are included in the Auto Attendant directory for the site. When you deploy a multisite Messaging environment, you can create a system wide Auto Attendant directory by selecting the name of the other site. You can click on a site to select the site. You can press the **Control** key and then click to select multiple sites. When you select the name of another site in this field, the system reaches the users who are in either directory through Auto Attendant for this site. If you change the selections in this field, you must reload the user list on all application servers for the site or wait for the nightly refresh for the changes to take effect.
Keypad entry	The keypad options: • **BASIC**: Enter extension only. • **ENHANCED**: Enter extension or spell name. If the **Speech recognition** field equals *enabled*, both options include speech recognition.
Speech recognition	The option to configure speech recognition. The default is *disabled*. Do not enable this feature unless your Messaging system includes a mainstream license. When you enable speech recognition, callers can say a name that is in the Auto Attendant directory and the Auto Attendant transfers the call to that person.
Auto Attendant Greeting / Menu	
Initial greeting	The initial greeting that Auto Attendant plays to a caller. You can browse to a prerecorded .wav file. After you upload a recording, you cannot change back to the system recording.
Menu (speech recognition disabled):	The menu that Auto Attendant plays when you set the **Speech recognition** field to *disabled*.
Menu (speech recognition enabled):	The menu that Auto Attendant plays when you set the **Speech recognition** field to *enabled*.

Initial topology administration

Overview for administering topology

The topology of a Messaging system is the relationship between the application servers and the sites that the topology supports. You can define this relationship on the Topology Web page. Use the Topology Web page to:

- List the sites that you previously defined on the Sites Web page.
- Assign an application server to a site.
- Change the topology by adding or deleting application servers.
- Configure the storage server role as primary or backup.

You must define topology properties on the storage server, which then applies these properties to the associated application servers.

- In a single-server topology, you can manage application and storage roles on the same server.
- In a front-end or back-end topology, you can manage all application roles on the server that has been assigned the storage role. The location of the application servers, relative to the storage server, can be local or remote.

If you configure a server to be an application-only server, the navigation pane displays a subset of the administration options. You cannot open storage-role Web pages from the navigation pane of a dedicated application server. To open storage-role Web pages, you must gain access to the storage server.

Application clusters:

You can combine up to four application servers to form a cluster. Each cluster connects to one storage server and supports the same telephony server. You must configure all cluster members for the same site.

By clustering application servers, you can:

- Increase the system capacity so the application server can support more users. Every application server you add to the cluster increases the number of available ports.
- Provide redundancy for any application server in the same cluster. You configure application servers within a cluster identically and are, therefore, interchangeable.

Important:

All servers in a cluster must be in the same time zone. If your organization spans multiple time zones and if your system topology includes application server clusters, then you need to configure one cluster for each time zone.

Mutare Message Mirror™

Messaging interoperates with Message Mirror to achieve a complete disaster recovery of voice messages and related information like greetings, names, passwords, and LDAP data.

You can setup a backup storage server. Message Mirror continuously monitors the message store and copies or *mirrors* messages, names, greetings, passwords, and LDAP changes to a backup message store.

For more information, see *Chapter 19: Redundant Message Store*.

Adding the first application server

Use this procedure to create a relationship between a site and:

- The only application server for the site.
- The first of several application servers for the site.

Complete this procedure on the storage server.

Note:

Only assign *one* site to an application server.

Before you begin

- Configure the storage and one or more application servers. See *Chapter 3: Initial administration of the storage role* and *Chapter 4: Initial administration of the application role*.
- Create a site with one or more application servers. See Overview for administering sites on page 82.
- Ensure that all application servers that you plan to add to the topology are running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**.
2. When the Topology Web page opens for the first time, the IP address defaults to the IP address of the storage server. Delete this IP address as follows:

a. In the **Remove Application Server** area, select the IP address for the storage server from the drop-down list.
b. Click **Remove**.

3. In the **Add Application Server** area:
   a. In the **IP address** field, enter the IP address of the first application server.
   b. In the **Add the server with** field, select **No active site configuration** .
   c. Click **Add**.
4. In the **Sites / Application Servers** area, select **Active** from the drop-down list next to the site that the application server supports.
5. Click **Update**.
   The system displays a confirmation message.
6. Click **OK** to proceed.
7. Restart Messaging.
   For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Example

The following table is an example of a complete distributed topology with two sites, Atlanta and Boston. Atlanta has two application servers and Boston has one.

Sites / Application Servers

Sites	10.200.0.2	10.200.0.3	10.210.0.1
Atlanta	Active	Active	-
Boston	-	-	Active

Next steps

- If there is only one application server on your site, you are ready to administer users on the system.
- If there are several application servers on your site, you must add the application servers to the system topology so that these application servers recognize each other. See Adding additional application servers on page 97.

Adding additional application servers

You must add application servers to a cluster from a storage server.

Before you begin

- Install and configure all application servers that you plan to associate with the site. See *Chapter 4: Initial administration of the application role*.
- Add the first application server to the site. See Adding the first application server on page 96.
- Ensure that all application servers that you plan to add to the topology are running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**.
2. In the **Add Application Server** area:
   a. In the **IP address** field, enter the IP address of the application server you are joining to the cluster.
   b. In the **Add the server with** field, select **The same site configuration as an existing application server:**
   c. From the drop-down list, select the application server that you want to join.

      All application servers in a site are identical. Hence, you can select any server from the list.

      You can join up to four application servers to form a site. However, you must configure all servers in a site to use the same time zone.
3. Click **Add**.
   The system:
   - Adds the server you identified in Step 2a in the **Sites / Application Servers** area.
   - Copies the site properties from the application server that you selected in Step 2c to the server you identified in Step 2a.
4. Repeat Step 2 and Step 3 for each application server that you want to add to the site.
5. Click **Update**.
   The system displays a confirmation message.
6. Click **OK** to proceed.
7. Restart Messaging.

   For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Next steps

Configure a cluster of application servers. See Configuring a cluster on page 99.

Changing the storage server role

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**.
2. In the **Role of the Server** field, select one of the following:
   - **Primary**
   - **Backup**
3. Click **Change**.
   The system displays a confirmation message.
4. Click **OK** to proceed.
5. Restart Messaging.
   For more information, see Stopping Messaging on page 377 and Starting Messaging on page 377.

Configuring a cluster

You must add all the application servers that you joined into a cluster to the individual cluster lists of the servers. Using this list, the servers can recognize each other. You can configure these lists on each individual application server.

Before you begin

Define the application server as a member of the cluster. See Adding additional application servers on page 97.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **Cluster**.
2. In the **Number of member appliances in the cluster** field, enter the number of application servers in the cluster.
   The maximum number you can enter is 4.
   The number of **Member** fields in the **IP address of each appliance** area increase to match the number you entered.
3. In each **Member** field, enter the IP address of an application server in the cluster.

- For a new cluster member, add each of the other cluster members to the cluster list to which the cluster belongs.
- For each preexisting cluster member, add the new member to the cluster list to which the cluster belongs.

Do not change the information in the **Disk usage quota** field.

4. Click **Apply**.
   The system displays a confirmation message.
5. Click **OK** to proceed.

   Repeat these steps until you configure all the application servers for your sites.

Administering a load balancer in the Exchange Server CAS array

A network load balancer evenly distributes client requests to multiple Exchange Servers in the CAS array for scalability and high availability. By using the full CAS array capability, the network load balancer increases the efficiency and improves the use of the servers.

For more information about load balancing, see Network Load Balancing Technical Overview at the *Microsoft TechNet* website.

Before you begin

Before administering a load balancer in the Exchange Server CAS array:

- Configure the CAS array as the peer Exchange Server to ensure that Messaging sends all client requests through the CAS array.
- Ensure that you meet the following conditions for naming and administering the load balancer:

Naming	Administering
- The CAS array must have a DNS record. - The name of the CAS array must be identical to FQDN and fulfill the following Microsoft NetBIOS naming conventions: • Must contain less than 15 characters. • Must not contain a space between characters. • Must not contain a period (.) Microsoft does not follow the naming conventions for naming the CAS array. In the examples for administering a CAS	- Administer the idle timeout with the maximum supported value for the load balancer for TCP connections. - Enable round-robin balancing. - Disable sticky connections to ensure that the load balancing is performed. For the virtual IP, the load balancer vendor might require a different virtual IP: • If the virtual IP has a DNS record, administer the peer Exchange server as the host name. • If the virtual IP does not have a DNS record, update the *hosts* file with the

Naming	Administering
array, Microsoft has used names with periods (.).	virtual IP, the host name and FQDN of the CAS array. **Note:** - Different load balancer vendors use different terms to describe the administration options of a load balancer. Ensure that you contact the load balancer vendor for the specific options to configure the load balancer with the application servers that use MAPI. - Update the `hosts` file only for troubleshooting purposes and to identify reasons for problems with load balancing.

About this task

Perform the steps to stop the Messaging services through the Messaging SMI, and perform the steps to edit the `hosts` file through Windows Explorer.

Procedure

1. Stop the Messaging services that use MAPI.
2. Open Windows Explorer and navigate to `c:\Windows\System32\drivers\etc`.
3. Right-click the `hosts` file, and select **Edit**.
4. At the end of the `hosts` file, add the following lines with the appropriate values:

   `<IP address of the CAS array> <host name of the CAS array>`

   `<IP address of the CAS server> <FQDN of the CAS array>`
5. On the Start menu, open the command prompt and type the **`ipconfig/flushdns`** command.
6. Start the Messaging services that you stopped in Step 1 and verify that:
   - The TUI service is active.
   - The peer Exchange server is online.
   - The mailbox monitoring function is available.

Topology field descriptions

Name	Description
Sites / Application Servers	The section displays the following information about the sites that you created on the Sites Web page: • The name of the site. • The IP address of each application server associated with the storage server. • The application server that is associated with a site as the *active* or *inactive* or *shared* server. The system updates the section after you add or delete application servers.
Add Application Server	
IP address	The IP address of the application server that you want to add to Messaging.
Add the server with	The options are: • **No active site configuration**: Select this option to add the first application server to a site. • **The same site configuration as an existing application server:** Select this option to add an application server to a site that already has an existing application server associated with the site. You can add up to four application servers to a site. All application servers in a site are identical, so you can select any existing application server in the drop-down list that is associated with the site. Remember to cluster the added server with the existing ones. See Configuring a cluster on page 99.
Remove Application Server	
IP address	The IP address of the application server that you want to delete from the site.
Storage Server Role	
Role of the Server	The options are:

Name	Description
	• **Primary** • **Backup**

Cluster field descriptions

Settings	Description
Cluster Members	Any number from 1 through 4. The maximum number of application servers in a cluster is four.
IP address of each appliance	An IP address for each member in the cluster. The number of **Member** fields for entering IP addresses increase depending on the number you entered in the **Cluster Members** area.
Disk usage quota	This is an advanced setting. Consult your account representative before you enter data in this field.

Verifying the link to the AxC

After you set up your sites and topology, you must verify that the AxC connector can link to each application role in your topology. You can test this link by reloading the system caches with the following user information:

- User List
- Global Address List

If you have a multiserver configuration, complete this test on *each* server in the application role.

Before you begin

Check the Initial administration checklist for sites and topology on page 81 and complete Step 1 through Step 7.

Procedure

1. On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**.

2. In the **Reload Caches** area, click **Reload** for each of the following lists:
   - User List
   - Global Address List

   If the caches reload without error, the system connects the application role to the AxC and the storage role properly. If the system returns an error message, ensure that:
   - You have entered the IP address for the AxC correctly. See Changing the AxC IP address on page 70.
   - You have set up the topology correctly. See Overview for administering topology on page 95.
3. If required, repeat Step 1 and Step 2 to ensure that the caches reload without error.

   Repeat this procedure on each server with the application role.

Chapter 7: Managing servers

Storage servers

Adding a trusted server

Use the Add Trusted Server Web page to add trusted servers to the messaging network. The servers might include a Provision server, the Avaya Site Administration (ASA) server, or the Avaya one-X® Mobile server. The customer administrator adds these servers after the initial installation.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Storage)** > **Trusted Servers**.
2. On the Manage Trusted Servers Web page, click **Add a New Trusted Server**.
3. On the Add Trusted Server Web page, select a type of trusted server from the **Special Type** drop-down list.

   If you select a common type of trusted server, the system automatically populates some of the fields on the **Add Trusted Server** Web page.
4. Enter the appropriate information in the fields.

   For more information, see Add Trusted Server field descriptions on page 106.
5. Click **Save**.

Next steps

To view a summary of all the administered trusted servers on the Trusted Servers Web page, click **Display Report of Trusted Servers**.

Manage Trusted Servers field descriptions

Name	Description
Trusted Server	The name of each trusted server.
IP Addr/Name	The IP address or the machine name of each server depending on how you administered the server.
Service Name	The service name of the trusted server.

Add Trusted Server field descriptions

Name	Description
Trusted Server Name	The name of the server can include up to 64 characters and must start with a letter. The other characters can be letters, numbers, dashes (-), and underscores (_). This field is mandatory.
Password	The password that the server uses to connect to Messaging.
Confirm Password	Reconfirm the password.
Machine Name / IP Address	The host name or the IP address of the trusted server. • The host name must be the fully qualified domain name (FQDN). For example: *machine.location.company.com*. If you do not enter the FQDN, you must include the domain name in the **DNS Domain** field on the Network Configuration Web page. • Trusted servers that use the private LAN require a valid IP address.
Service Name	A descriptive name that indicates the use of this trusted server. The system automatically populates this field if you select a trusted server from the **Special Type** drop-down list.
Minutes of Inactivity Before Alarm	The number of minutes the trusted server can be inactive before the system raises a minor alarm. The default is 0. If you do not change the default, the system does not check for inactivity from this trusted server. The range is 0 to 1440.
Access to Cross Domain Delivery	Specifies whether you want to allow cross-domain delivery through this trusted server.

Name	Description
Special Type	The type of the trusted server. The system automatically populates or restricts some of the fields on the page based on your selection.
LDAP Access Allowed	Specifies whether you want the trusted server to have LDAP access to the storage server. The default is *yes*.
LDAP Connection Security	The type of encryption for the LDAP connection between the trusted server and the storage server. If the value in the **LDAP Access Allowed** field is *no*, the system disables this field. Select one of the following: • **Must use SSL**: For Secure Sockets Layer (SSL) encryption. SSL is the preferred encryption method because SSL provides full channel encryption. • **Must use SSL or encrypted SASL**: For SSL or Simple Authentication and Secure Layer (SASL) encryption. • **No encryption required**: This is the default value.
IMAP4 Super User Access Allowed	Specifies whether you want the IMAP4 super user to access the storage server from the trusted server. The default is *no*.
IMAP4 Super User Connection Security	The type of encryption for the IMAP4 super user connection between the trusted server and the storage server. If the value in the **IMAP4 Super User Access Allowed** field is *no*, the system disables this field. Select one of the following: • **Must use SSL**: For SSL encryption. SSL is the preferred encryption method because SSL provides full channel encryption. • **Must use SSL or encrypted SASL**: For SSL or SASL encryption. This is the default value.

Report of Trusted Servers field descriptions

Name	Description
Trusted Server Name	The name of each trusted server.
IP Address	The IP address of each trusted server.
Service Name	The service name of each trusted server.

Setting Messaging parameters

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Ports and Access**.
2. Enter the appropriate information in the fields.

   For more information, see System Ports and Access field descriptions on page 110.
3. Click **Save**.

Privacy enforcement

Messaging enforces the following levels of privacy for messages that are retrieved by IMAP4 and POP3 clients:

- *Voice* enforces privacy from the Telephone User Interface (TUI). If a caller marks a voice message as private, Messaging:
  - Blocks the recipient from using the TUI to forward the message.
  - Allows clients who accept the voice mail privacy to retrieve the message.
  - Blocks clients who do not accept the voice mail privacy from retrieving the message. Messaging replaces the blocked message with an informational message in the language that the user selected in User Preferences.
- *Email* requests that the recipient keep the message private. Recipients must enforce the privacy of the message. Messaging cannot enforce privacy rules on to clients who do not have the capability to mark messages as private. Most clients do not restrict the forwarding of private messages. However, IMAP4 clients typically do not retrieve the .wav attachment of a private message.

If there are users with an external message store such as Exchange, you cannot perform the following changes on the System Ports and Access Web page:

- Setting the value in the **Privacy Enforcement Level** field to a value other than *Email*
- Setting the value in the **Automatic Mail Forwarding** field to a value other than *yes*

Setting the privacy enforcement level for IMAP4 and POP3 clients

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Ports and Access**.
2. In the **System Attributes** area, select a value from the **Privacy Enforcement Level** field:
   - Voice
   - Email
3. Click **Save**.

Configuring IMAP4 access

Configure system-wide parameters on the System Ports and Access Web page. Use the following instructions to configure IMAP4 access to the storage server for remote email clients and if needed, for Avaya one-X products and provisioning tools.

Before you begin

Messaging must be running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Ports and Access**.
2. In the **System TCP/IP Ports** table, enable the following ports:
   - **IMAP4 Port**
   - **IMAP4 SSL Port**

   For more information, see System Ports and Access field descriptions on page 110.
3. Click **Save**.

System Ports and Access field descriptions

Fields	Description
SYSTEM ATTRIBUTES	
System Prime Time Start	The start time, in hours and minutes, for the prime time interval. This is usually the time that your company opens for business. The default is 08:00.
System Prime Time End	The end time, in hours and minutes, for the prime time interval. This is usually the time that your company closes for business. The default is 17:00.
Maximum Simultaneous LDAP Directory Update Sessions	The maximum number of simultaneous LDAP sessions that the system allows during a full remote update. When the system reaches the maximum, you cannot request a full remote update until one of the sessions finishes. The default is 100. The range is 0 to 100.
IMAP4 TUI Password	The password used for the IMAP4 communication between systems.
Confirm IMAP4 TUI Password	A confirmation of the password you enter in the **IMAP4 TUI Password** field.
Default Internet Subscriber Community	Do not use this field.
Privacy Enforcement Level	If the sender marks a message as private, then the recipient cannot forward the message from the TUI. The options are: • *Voice*: Enforces privacy from the TUI. • *Email*: Requests that the recipient keeps the message private. For Exchange message stores, the privacy enforcement level must be *Email*.
Automatic Mail Forwarding	For Exchange message stores, the value must be *yes*.
RESCHEDULING INCREMENTS FOR FULL MAILBOX DELIVERY	
Increment fields	The intervals in days, hours, and minutes that the system waits to attempt to resend messages that the system could not deliver

Fields	Description
	on the previous attempt due to a full mailbox. When the system uses the specified last increment, the message is marked as non-deliverable. You can specify a maximum of 10 rescheduling increments.
SYSTEM TCP/IP PORTS	
LDAP Port	The state of the primary LDAP port. You cannot change the primary port number. The options are: • *Disabled*: Disables authenticated and anonymous access for the corporate LAN. • *Authenticated Only* : Authenticates access and disables anonymous access on the corporate LAN. • *Authenticated or Anonymous*: Authenticates access or anonymous access on the corporate LAN. Changing the state of the LDAP port temporarily interrupts the corporate LAN access to LDAP.
LDAP SSL Port	The port number for the LDAP SSL port. The default is 636. If you change the port number, you must restart the system.
LDAP Front End Alternate Port	An optional, secondary port for LDAP. When you enter a port number, the system automatically enables the port. The default is blank. If you change the port number, you must restart the system.
LDAP Directory Update Port	The port that the directory update LDAP server uses. The default is 56389.
IMAP4 TUI Port	You cannot change the status of this port. The port is disabled and the port number is 55143.
IMAP4 Port	The port that the IMAP4 server uses for IMAP4 communication with remote clients. If you select *Enabled*, enter the port number that the IMAP4 server uses.

Fields	Description
IMAP4 SSL Port	The port that the IMAP4 server uses for IMAP4 SSL communication with remote clients. If you select *Enabled*, enter the port number that the IMAP4 server uses. The default is 993.
POP3 Port	The port that the POP3 server uses for POP3 communication with remote clients. The options are: • *Enabled*: Allows the use of POP3 clients for email messaging. • *Disabled*: Blocks POP3 email client access to the messaging server. If you select *Enabled*, enter the port number that the POP3 server uses for POP3 communication with remote clients. The default is 110.
POP3 SSL Port	The port that the POP3 server uses for POP3 SSL communication with remote clients. The options are: • *Enabled* allows POP3 clients to use the POP3 SSL port for more secure access. • *Disabled* blocks POP3 SSL client access. If you select *Enabled*, enter the port number that the POP3 server uses for POP3 SSL communication with remote clients. If you enable POP3 SSL, users must configure their email clients to use SSL. The default is 995.
SMTP Port	The port that the SMTP server users for SMTP communication with remote clients. If you select *Enabled*, enter the port number that the SMTP server uses. The default is 25. Disabling this port only disables access to the public LAN. If you change the port number, you must restart the system.
SMTP Alternate Port	The port that the SMTP server uses for SMTP communication with remote clients. Use this additional port on the public network instead of the traditional SMTP port. The system automatically enables this port when you enter a port number. The default is blank.

Fields	Description
SMTP SSL Port	The port that the SMTP server uses for SMTP SSL communication with remote clients. If you select *Enabled*, enter the port number that the SMTP server uses for SMTP SSL communication. The default is 465. If you change the port number, you must restart the system. If you enable SMTP SSL, users must configure their email clients to use SSL.
Allow TLS for Outgoing SMTP	Outgoing SMTP attempts to use Transport Layer Security (TLS) to encrypt the SMTP conversation.
MCAPI Port	The port that the MCAPI server uses. The default is 55000. If you change the port number, you must restart the system.

Adding a network server

Use the Networked Servers Web page to connect Messaging to a different network environment. For example, a Message Networking environment.

About this task

The following steps are for adding an LDAP server.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Storage)** > **Networked Servers**.
2. On the Manage Networked Servers Web page, select an LDAP server.
3. Click **Add a New Networked Server**.
4. On the Add Networked Machine Web page, enter the appropriate information in the fields.

   For more information, see Add Networked Machine field descriptions on page 114.
5. Click **Save**.

Next steps

- To view a summary of the local and networked machines that are administered on the Networked Servers Web page, click **Display Report of Servers**.
- To view the networked machines on the Networked Servers Web page, click **Display Network Snapshot**.
- To view a summary of the local and networked servers and their respective extension ranges on the Networked Servers Web page, click **Display Report of Server Ranges**.

Manage Networked Servers field descriptions

Name	Description
Server Name	The name of the network server.
IP Address	The IP address of the network server.
Server Type	The type of server. For all machines except the local machine, the server type is LDAP.
ID	The numerical identification of the server.
Total Subs	The number of users associated with the network server.

Add Networked Machine field descriptions

Name	Description
Machine Name	The name of the server that you want to add.
Password	The password used for directory updates.
Confirm Password	Confirm the password that you entered in the **Password** field.
IP Address	The IP address of the server that you want to add.
Machine Type	The server type for the server you want to add. For all machines except the local machine, the server type is LDAP.
Mailbox Number Length	The length of the long or global mailbox number.

Name	Description
	The Mailbox Number Length must be comma-separated numbers. There must be no spaces and each number must be between 2 and 50 only.
Default Community	Do not use this field.
Updates In	Specifies whether the local server accepts directory updates from the network server. If you are administering the local server, this field controls updates on a system-wide basis. The options are: • *yes*: Accepts directory updates from network servers. • *no*: Blocks directory updates to the sever, regardless of the setting of the field for the network server.
Updates Out	Specifies whether the local server can send updates about users to the specified remote server. If you are administering the local server, this field controls updates on a system-wide basis.
Remote LDAP Port	The port that the system uses to connect to the network server to send directory updates. The default is the port that you specify in the **LDAP Directory Update Port** field on the System Ports and Access Web page.
Inbound LDAP Security	The type of encryption required for the connection between the storage server and a remote network server for inbound LDAP directory updates. When you set the **Updates In** field to *no*, the system denies any attempt by a remote network server to update the LDAP directory without using the specified level of security. The options are: • *Must use SSL*: Requires SSL encryption for inbound LDAP directory updates. • *Must use SSL or encrypted SASL*: Requires either SASL or SSL encryption for inbound LDAP directory updates . The default value is *Must use SSL or encrypted SASL*.

Name	Description
Outbound SMTP Port	The port the system uses to connect to this network server. The defaults are port 25 for SMTP and port 465 for Secure SMTP.
Outbound SMTP Service	The type of SMTP service required for the connection between the storage server and a remote network server. Choices are SMTP or Secure SMTP.
MAILBOX NUMBER RANGES *The total length of the prefix and the mailbox number must not exceed 64 digits.*	
Prefix	The prefix for the range of telephone numbers for users on the server. The system uses the prefix to distinguish between servers that have overlapping ranges for mailbox numbers.
Starting Mailbox Number	The first number in the range for mailbox numbers on this server. The number of digits in the range must match the entry in the **Mailbox Number Length** field. Unless you have a specific reason for excluding some ranges, start with 1 preceded by leading zeros. Example of a five-digit number: *00001*.
Ending Mailbox Number	The last number in the range for mailbox numbers on this server. Example of a five-digit number: *99999*.
Telephone Number Mapping *When a local user receives a call-answer message, the system attempts to match the sender calling party number (CPN) to a user number in the database.*	
Enable Telephone Number Mapping	The options are: • *yes*: Use a lookup table to map the CPN of the sender to the number of the recipient. • *no*: Instructs the system not to identify the recipients as users in the Messaging network. If you change this option from *yes* to *no*, the system deletes all previously defined mapping from the local database. The system also sets the telephone numbers for all existing users associated with the network server to null.

Comments? infodev@avaya.com

Name	Description
Map From	The system compares the digit string that you enter in this field to the base numbers for a user. A match occurs when the value in the **Map From** field is the same as the initial digits of the base number. If this happens, the system creates a mapped telephone number by: • Stripping the matching digits from the base number • Prepending the number in the **Map To** field to the base number. If the **Map From** field is empty, the system compares incoming CPNs to all base numbers. Valid values are digits from 0 through 50. You can add more than one set of Map From and Map To numbers. If you add more than one set, the sets can differ in length.
Map To	The digits string that the system prepends to the base number after the system strips the digits that match the **Map From** field. When the **Map To** field is: • Empty: The system does not prepend digits to the base number after digit stripping. • *none*: The system sets the matching telephone number to null. The **Map To** entries can be of different lengths. The resulting telephone numbers must not be longer than 50 digits.
Add Mapping	The mapping to add to the mapping table.
Delete Mapping	The mapping to delete from the mapping table. To change an existing mapping, delete the mapping and then create a new mapping.

Report of Network Servers field descriptions

Name	Description
Server Name	The name of each network server.

Name	Description
IP Address	The IP address of each network server.
Server Type	The type of network server. For all servers except the local server, the server type is LDAP.
LDAP Port	The LDAP port used for directory updates.
Updates In	The current setting for allowing directory updates from the network server to the local server.
Updates Out	The current setting for allowing directory updates from the local server to the network server.
Total Subscribers	The current count of users associated with the server.

Network Snapshot field descriptions

The report displays information about the existing network servers and the current state of their connections. The report is display only.

Name	Description
Log Start Date	The date of the first entry in the log used to generate the report.
Log End Date	The date of the last entry in the log used to generate the report.
Machine Name	The name of each server in the network. To change the data for a server, click the name.
Last Connection	The date and time of the last connection. • **Outgoing Connections**: Displays the last time the local server connected to the remote server. • **Incoming Connections**: Displays the last time the remote server connected to the local server.
Status	The status of the last connection.
Retries	The number of consecutive times that the local server tried, but failed to connect to the remote server.

Report of Server Ranges field descriptions

Name	Description
Server Name	The name of each server in the network. To change the data for a server, click the name.
Prefix	The address prefix of each server range.
Starting Mailbox Number	The first mailbox number in the range.
Ending Mailbox Number	The last mailbox number in the range.

Application servers

If you configure a server to be an application-only server, the navigation pane displays a subset of the administration options. You cannot open storage-role Web pages from the navigation pane of a dedicated application server.

To open storage-role Web pages, you must gain access to the storage server.

Dial Rules field descriptions

Warning:

If you are currently using dial rules based on the application server, you must manually migrate to use the site-based dial rules, as the future Messaging release will not support dial rules based on the application server. For more information, see Migrating dial plan data from R6.0.1 SP3 or R6.1 to R6.2 on page 84.

Name	Description
Dial Plan Handling	
Dial plan handling style	The options are: • Application server based: This is the Messaging 6.0 legacy style, which is deprecated. • Site definition based: Use site-based dial rules to perform dial rules tests from within the storage server. This is the default option.

Name	Description
Dial plan handling testing	Click **Test** to verify whether the phone numbers are handled correctly.
This Location	
Country code	The country code of the dialing phone number. Use this number to determine whether the calls are internal, local, domestic, or international. This field is deprecated. Use the **Country code** field on the Sites Web page.
Area code	The area code of the dialing phone number. Example: *212 -5551212* The system uses the area code to determine if the outgoing calls are local or long distance. This field is deprecated. Use the **National destination code** field on the Sites Web page.
Dial-Out Settings	
Long-distance prefix	The preceding digits before the area code of the dialing phone number. The default is 1. This field is deprecated. Use the **National prefix** field on the Sites Web page.
International prefix	The preceding digits before the country code of the dialing phone number. The default is 011. This field is deprecated. Use the **International prefix** field on the Sites Web page.
Outside line prefix	The digits required to gain outside line access. The default is 9. This field is deprecated. Use the **Outside line prefix** field on the Sites Web page.
Company DID numbers that should be treated as internal numbers	
Number of digits in an extension	This field is deprecated. If you are configuring an: • External (Public Network) Dial Plan Site, configure the length of digits required to call a number within the originating area code or a local call in the **Subscriber**

Name	Description
	number length (within this site's national destination code) field. • Internal Dial Plan Site, configure the length of extensions for users on this site in the **Short extension length** field.
Number of DID ranges	The number of Direct Inward Dialing (DID) ranges for internal numbers. The system uses the DID range to route inbound calls to extensions within the bounds of the range. This field is deprecated.
PBX Caller ID Information	
Caller ID internal number prefix	The dial-out prefix for internal calls. The system uses this field only when required by the telephony server for caller ID. This field is deprecated.
Advanced Rules	
Advanced Dial-out rules	Click **Edit Dial-Out Rules** to customize the dial-out rules. Use the fields under the Toll-Free and Premium Calls section and the Local Calls section on the Sites Web page to configure the dial-out rules.
Dial-in rules	Do not change the advanced dial-in rules unless Avaya Client Services directs you to change the rules.

Dial Plan Handling Test field descriptions

Name	Description
Dial-Out Test Numbers	Use this section to define phone numbers to verify whether the Dial-Out Rules script handles these numbers correctly. You can also use this section to troubleshoot out-dialing problems and to verify that a given phone number is classified and dialed correctly. Define phone numbers, one per line, as these phone numbers would appear in the

Name	Description
	directory or as users would enter these phone numbers, for example, in the Mobile phone field, the Personal attendant field, the Reach Me settings, or the Notify Me settings. Click **Test** to test the numbers.
Dial-Out Test Results	This section includes information on the input phone number, the call type, and the output phone number. The call type could be internal, long distance, international, or invalid.
Dial-Out Script Configuration	This section includes the dial-out script configuration information. The configuration data includes the country code, area code prefix, area code, extension length, and so on.

Dial-Out Rules field descriptions

Name	Description
Dial-Out Rules Script	This script performs the dial plan handling using various parameters as specified in the site definitions for those sites handled by this application server. Do not modify this script unless explicitly mandated by Avaya.
Dial-Out Test Numbers	Use this section to define phone numbers to verify whether the Dial-Out Rules script handles these numbers correctly. You can also use this section to troubleshoot out-dialing problems and to verify that a given phone number is classified and dialed correctly. Define phone numbers, one per line, as these phone numbers would appear in the directory or as users would enter these phone numbers, for example, in the Mobile phone field, the Personal attendant field, the Reach Me settings, or the Notify Me settings. Click **Test** to test the numbers.

Name	Description
Dial-Out Test Results	This section includes information on the input phone number, the call type, and the output phone number. The call type could be internal, long distance, international, or invalid.
Dial-Out Script Configuration	This section includes the dial-out script configuration information. The configuration data includes the country code, area code prefix, area code, extension length, and so on.

Dial-In Rules field descriptions

Name	Description
Dial-In Rules Script	The system identifies mailboxes by the extension of the user. However, for various reasons like inter-site routing or other special configurations, the PBX passes the extension preceded by additional digits to the appliance. For the system to process the call correctly, the system strips the leading digits off using a dial-in rule. Otherwise, the system does not recognize the extension and transfers the call to the voice mail pilot greeting. Do not modify this script unless explicitly mandated by Avaya.
Dial-In Test Numbers	Use this section to define phone numbers and names to verify whether the Dial-In Rules script handles these correctly. Each line must have one Called ID, one Caller ID, and a Caller Name, each separated with a comma. Names can contain commas, but phone numbers cannot contain commas. Click **Test** to test the phone numbers and names.
Dial-In Test Results	This section includes information on the Called ID, the Caller ID, the Caller Name, and the Result.

Fax overview

You can receive an incoming fax using any of the following methods:

- **Receive and forward to email**: The Messaging system acts like a fax server and hence you do not need a third-party fax server. If the recipient user belongs to a CoS that allows fax, the user receives the fax in the inbox of the configured email address.
- **Detect and transfer to fax server**: If the recipient user belongs to a CoS that allows fax, the user receives the fax through the user fax server account.

Inbound fax limitations

The maximum transmission length for an incoming fax is 90 minutes. However, if the fax transmission exceeds the 90-minutes limit, the system handles the fax messages gracefully, that is, the system stops the fax transmission. The fax message to the user contains the pages sent in the first 90 minutes of the transmission, and the system notifies the sending fax machine of the number of pages sent successfully.

Nightly maintenance

You can schedule the time for nightly maintenance of each application server on the System Parameters Web page. During the nightly maintenance, the Messaging system reloads the user list and GAL on each application server.

Currently, the nightly refresh of users runs on all application servers at the same time. You must stagger this activity across application servers.

Message recording

Use the **Maximum Message Length** field on the System Mailboxes Web page to define the number of minutes or megabytes of the longest message that a user can create on the Messaging system. The default value is 100 minutes. This is a system-wide setting that applies to all users. However, if you want to set additional restrictions for your users, you can do so using the Class of Service Web page.

Use the **Maximum voice message length** field on the System Parameters Web page to define the maximum time for a message recording in seconds. The default value is 1200 seconds, that is, 20 minutes. The maximum value you can enter in this field is 4500 seconds, that is, 75 minutes. The value you specify in the **Maximum call answer message length** field on the Class of Service Web page must not exceed the value you specify in the System Parameters Web page.

Configuring system parameters

System parameters include call handling parameters such as caller ID, Call Sender options, message recording times, ring-no-answer timeouts, Reach Me options, ringback timeouts, and fax server integration.

You can preset all these parameters with default values, and generally, the system invokes these defaults without further modification requirements. However, as an administrator, you can change these parameters, if necessary. If you change the parameters, ensure that you repeat the changes on each application role in the cluster.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **System Parameters**.
2. Enter the appropriate information in the fields as described in System Parameters field descriptions on page 125.
3. Click **Apply**.
   The system displays a confirmation dialog.
4. Click **OK** to proceed.
   Repeat this procedure on each application role in the cluster.

System Parameters field descriptions

Name	Description
Avaya Branding Tone	The Messaging system plays the Avaya branding tone when a user logs in to the user mailbox. The options are: • **enabled** • **disabled** By default, the Messaging system enables the Avaya branding tone.
Voice Messages	
Include caller ID in subject line	The options are:

Name	Description
	• **enabled** (default): Includes the caller ID in the subject line of voice messages. • **disabled**: Excludes the caller ID in the subject line. Select *Disabled* only when the telephony server integration does not support the caller ID.
Intro text in subject line of original messages **Intro text in subject line of message replies** **Intro text in subject line of forwarded messages**	The text content prefixes the subject line of voice messages. The type of prefix that the system uses depends on the message context: • Original messages • Message replies • Forwarded messages The text content is the caller ID and contact name.
Call Sender	
For internal calls, a call attempt times out after	The number of seconds that elapse before the telephony server sends an internal call initiated from Call Sender to voice mail. The default is 16 seconds. The value must be less than the time taken by a call to a local extension to roll over to voice mail in RNA. If you configure the time out value at the system level on the telephony server, you will be able to check your telephony server for a typical setting.
For external calls, a call attempt times out after	The number of seconds that elapse before the telephony server sends an external call initiated from Call Sender to voice mail. The default is 45 seconds. During Call Sender initiated calls, to avoid a call going to voice mail, the time out value for Call Sender must be lower than the time taken by a call to an external telephone number to roll over to voice mail in RNA cases.
Maximum duration of a Call Sender initiated call	The maximum duration of a call, in seconds, when placing a call using Call Sender. The default is 10800 seconds, that is, 3 hours.
Recording Times	
Maximum voice message length	The maximum time for a message recording measured in seconds. The default is 1200 seconds, that is, 20 minutes.

Name	Description
	The maximum value you can enter is 4500 seconds, that is, 75 minutes.
End-of-recording silence	The seconds of silence that indicate the end of recording. The default is 4 seconds.
VoIP DTMF cut-off time	For VoIP integrations only. The number of milliseconds to cut off at the end of a recording that has been terminated by DTMF. The default is 150 milliseconds.
Play on Phone	
Time out (on no answer) after	If you do not answer a Play on Phone call in the specified time, in milliseconds, the system terminates the call. Choose a duration that is one ring less than the number of rings for call forwarding defined on the telephony server. The default is 16000 milliseconds and the maximum is 999999999 milliseconds.
Reach Me	
Number of seconds per ring for "Reach Me"	For the Reach Me feature, the number of seconds a ring is presumed to take when calculating how long to wait before timing out. The default is 5 seconds. You can manage how the system forwards your incoming calls using the Reach Me configuration options.
Ringback Timeouts	
First ringback timeout	The time to wait, in milliseconds, for the first ringback. The default is 15000 milliseconds.
Ringback timeout	The time to wait, in milliseconds, for the ringback to end. The default is 7000 milliseconds.
Nightly Maintenance	
Maintenance time	The scheduled time of nightly maintenance for each application server. During maintenance time, the system refreshes the local directory cache on the application server with a fresh copy of the directory cache.
Caller Access to System Main Menu	

Name	Description
Allow callers to reach the system main menu	The option to allow a caller to leave a call answering session by pressing the asterisk (*) button and gain access to the system main menu. The caller can connect to other extension numbers from the system main menu. The options are: • yes: When you set this value, if a caller dials an extension number that is busy or does not respond, the call is forwarded to the Messaging access number. If the extension number where the call is forwarded does not have an associated mailbox or a caller application, Messaging answers the call and plays the Messaging access greeting. • no: When you set this value, if a caller dials an extension number that is busy or does not respond, the call is forwarded to the Messaging access number. If the extension number where the call is forwarded does not have an associated mailbox or a caller application, Messaging disconnects the call. The default is *yes*. This field is applicable only to users of the Aria TUI.
Fax	
Fax receiving	The fax method to use for receiving an incoming fax. The options are: • **Detect and transfer to fax server**: If the recipient user belongs to a CoS that allows fax, then the user receives the fax through the user fax server account. • **Receive and forward to email**: If the recipient user belongs to a CoS that allows fax, then the fax is received in the inbox of the configured email address.
Fax detection time-out	The duration, in milliseconds, that the application server listens to possible fax tones after accepting a call. The default is 40000. If you configure a site with multiple languages and a user has long greetings, these could add up to exceed the 40 seconds fax time-out duration. In this scenario, if

Name	Description
	someone tries to send a fax to the user, waits for the entire prompt to finish, and hits the send button on the fax, the fax will not meet the 40 seconds time-out duration. In such scenarios, you must adjust the time-out duration even longer.
Intro text in subject line of Fax messages	The text that is present in the subject line of fax messages. This field is available only if you set the **Fax receiving** option as **Receive and forward to email**.
Fax recording format	The format for the fax recording. The options are: • **PDF (Portable Document Format)**: When the system records and sends an incoming fax to a user, the attached fax message is a PDF file. You can use the Adobe PDF viewer or any other supported programs to view the attached file. The default format is PDF. • **TIFF (Tagged Image File Format)**: When the system records and sends an incoming fax to a user, the attached fax message is a TIFF file. You can use the Windows Picture and Fax Viewer or any other supported programs to view the attached file. This field is available only if you set the **Fax receiving** option as **Receive and forward to email**.
Fax Server pilot number	The number, usually a hunt group number, of the third party fax server to which the system forwards the faxes. This field is available only if you set the **Fax receiving** option as **Detect and transfer to fax server**.
Destination identification during transfer	The fax destination for fax recipient, which is a mailbox or a primary extension. The default is Mailbox. This field is available only if you set the **Fax receiving** option as **Detect and transfer to fax server**.
DTMF following destination identification	The field can be none (), asterisk (*), or hash (#). The default is none.

Name	Description
	This field is available only if you set the **Fax receiving** option as **Detect and transfer to fax server**.

Changing the configuration of a cluster

About this task

Use the following steps to add or delete servers with the application role from an existing cluster. To set up a cluster for the first time, see Configuring a cluster on page 99.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **Cluster**.
2. Enter the appropriate information in the fields.
   For more information, see Cluster field descriptions on page 103.
3. Click **Apply**.
   The system displays a confirmation message.
4. Click **OK** to proceed.

Configuring storage capacity for offline call answering

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **Cluster**.
2. In the **Disk usage quota** field, enter the information in bytes.
   The default is *80 GB*.

   Note:

   This is an advanced setting. You must consult your account representative before you enter information in this field.
3. Click **Apply**.
   The system displays a confirmation message.
4. Click **OK** to proceed.

5. On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **Miscellaneous**.
6. In the **Delete cached voice messages from the cache after** field, enter the time in hours.

   The default is *72 hours*.

   If you increase the default time in the **Delete cached voice messages from the cache after** field without increasing the value in the **Disk usage quota** field, you could fill up the default quota of 80 GB.

   To prevent this, you must check your current usage.
7. On the **Administration** menu, click **Messaging** > **Server Information** > **Cache Statistics (Application)**.

   Check the *Storage Usage* section. You can view the percentage of storage used and your disk usage quota.
8. Click **Apply**.
   The system displays a confirmation message.
9. Click **OK** to proceed.

External servers

Changing external SMTP hosts

About this task

When you administer the storage role for the first time, you integrate Messaging with an external SMTP host server and a mail gateway. The external SMTP host forwards outbound email and is required to support notifications. Using the mail gateway, you can enable Messaging to connect to other mail systems.

When you change the external SMTP server, you must also update the mail gateway.

Procedure

1. To change the external SMTP host server, see Administering the external SMTP host on page 41.
2. To change the mail gateway, see Adding a mailbox gateway on page 42.

Chapter 8: Managing users

User overview

You can manage users only using the storage server SMI, and not the application server SMI. If you configure a server to be an application-only server, the navigation pane displays a subset of the administration options. You cannot open storage-role Web pages from the navigation pane.

To open storage-role Web pages, you must gain access to the storage server.

Users are subscribers with voice messaging capability.

- *Local* users are served from the same Messaging system, regardless of the location of their home telephony server. You use the User Management Web page to add, change, or delete a local user or an info mailbox.
- *Remote* users are served by a voice mail domain that is different from the voice mail domain of the local users. You must regularly update the list of remote users on your system to keep the system functioning properly.

Both local and remote users are members of the same voice mail network within your organization. Usually, local and remote users exchange messages with each other regularly.

User options for responding to messages

Users have the following options to respond to Call Answer messages from local or remote users:

- Send a reply message.
- Call the user who left the message.
- Generate an email response to the message if the user enabled Notify Me.

The options depend on how you:

- Administer dial rules for local users.
- Set up the mapping tables that enable your local system to recognize remote users.
- Coordinate remote updates with the administrators of remote systems.

Dial rules

Dial rules determine how local users can respond to messages from callers. Different rules apply to remote users and to callers who are not members of your organization. For example,

local users might be able to return a call from a remote user by replying to a Call Answer message. However, local users must dial the telephone number of the callers who are not members of your organization.

Your local Messaging system must identify remote users so that the Messaging system can apply dial rules correctly and retrieve directory information about the user.

For more information on dial rules, see Defining dial rules on page 85.

Mapping tables

Use the mapping tables to enable your local system to send messages from a local user to a remote extension. The system uses the mapping tables to change the telephony server extensions or network addresses of remote users to telephone numbers that your local system can recognize. The system then shares these telephone numbers between all messaging systems in your voice mail network.

Messaging systems use the telephone numbers to identify the callers over the network. For example, when a local user receives a call from a remote user, the system uses the telephone number to retrieve information regarding the caller.

You can create mapping tables when you add a network server to your system. See Adding a network server on page 113.

Remote updates

Your local system maintains a list of remote users. Remote updates keep this list up to date.

As the administrator of your local system, you must ensure that the administrator for each remote system in your voice mail network agrees to allow remote updates from your local system. You must then update the list of remote users on your local system regularly.

For more information, see Remote updates on page 152.

Manage local users

Adding users

Use this task to add users to the Messaging system. You can select any of the configured storage destinations for your messages.

If you have users that are already created in Active Directory, you can add these users directly to the Messaging system without having to manually configure the user values. For more information, see Adding users from Active Directory on page 135.

You cannot add users if the storage destination is Exchange and any of the following conditions are true on the System Ports and Access Web page:

- The value in the **Privacy Enforcement Level** field is *Voice*
- The value in the **Automatic Mail Forwarding** field is *no*

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. In the **Add a new user** area on the User Management Web page, click **Add**.
3. Enter the appropriate information in the fields.

   For more information, see User Management Properties field descriptions on page 139.
4. Click **Save**.

   If appropriate, you can designate the user as an attendant. See Assigning an attendant number on page 86.
5. Repeat Step 2 through Step 4 for each additional user.
6. Notify the new users that the Messaging service is available.

Adding users from Active Directory

Use this task to add users that are already created in Active Directory to the Messaging system.

You cannot add users if the storage destination is Exchange and any of the following conditions are true on the System Ports and Access Web page:

- The value in the **Privacy Enforcement Level** field is *Voice*
- The value in the **Automatic Mail Forwarding** field is *no*

Before you begin

- You have configured the Exchange storage destination. For more information, see Configuring a storage destination on page 52.
- Active Directory must include the user that you want to add to the Messaging system.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.

2. In the **Add User by AD Lookup** area on the User Management Web page, select any of the following from the Active Directory field name drop-down list:
   - mail: Select this option and enter a valid Active Directory account e-mail address in the text field.
   - telephone number: Select this option and enter a valid Active Directory account phone number in the text field.

     The system uses the phone number to determine the site for the user based on the site dial plan.
   - name: Select this option and enter a valid Active Directory account name in the text field.

   For more information, see User Management field descriptions on page 138.
3. Click **Look Up** to perform a search in Active Directory.
   - If a Messaging mailbox exists for the search result, the system displays a message stating that Mailbox *mailbox number* already exists for the user that you want to add.
   - If the system displays multiple users on lookup, you must refine the results such that the system displays a unique user.
   - If the system displays a single user with no existing Messaging mailbox as the search result, click **Add** to add the user in the Messaging system.

     At a minimum, Active Directory must include the Mailbox and Voice mail extension details for the user that you want to add.
4. Notify the new users that the Messaging service is available.

   The default password for the new users is 12345.

Changing user properties

About this task

You can view and change the properties of users present in the Messaging system.

You can change a user name or extension without disrupting mailing lists. For example, if Jane Doe is on a mailing list and her name changes to Jane Smith, Messaging automatically updates the list. A unique, system-generated user ID, and not the name or extension, links the user mailbox to lists and personal directories. You cannot access this system-generated ID.

You cannot change the user properties if the storage destination is Exchange and any of the following conditions are true on the System Ports and Access Web page:

- The value in the **Privacy Enforcement Level** field is *Voice*
- The value in the **Automatic Mail Forwarding** field is *no*

Procedure

1. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.
2. Use the built-in filters to locate the user you want to edit and then click the appropriate **Mailbox** number.

   You can also change user properties from the User Management Web page. However, this page does not have filters that assist you in locating a specific user.
3. On the User Management > Properties Web page, change the user information as appropriate.

   For more information, see User Management Properties field descriptions on page 139.
4. Click **Save**.
   The system saves the user properties.

Deleting users

Procedure

1. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.
2. Use the built-in filters to locate the user that you want to delete and then click the appropriate **Mailbox** number.

   You can also delete users from the User Management Web page. However, the User Management Web page does not have filters that assist you in locating a specific user.
3. On the User Management > Properties Web page, click **Delete**.

   For information about the fields, see User Management Properties field descriptions on page 139.
4. In the confirmation screen, click **OK** to continue.
   The system deletes the user.

Speech recognition

The name of a user, info mailbox, or distribution list might not follow the pronunciation rules of the primary language for your system. To increase the likelihood that the speech recognition feature recognizes the name, you can spell the name the way you would pronounce the name.

Speech recognition in both Speech Auto Attendant and Speech Enabled Message Addressing uses the following fields:

- **First name** + **Last name**
- **Display name**
- **Pronounceable name**

There is no search order between these fields. A match is a match. You must use the **Pronounceable name** field to increase speech recognition. However, you can use the other fields to increase the recognition rate.

For example, if the primary language of your system is English, spell Dan DuBois as `Dan Doobwah`.

You can also enter an alternative name for the user. For example, William Bell might also be known as Bill Bell. In the User Properties Web page, if you enter `William` in the **First name** field, `Bell` in the **Last name** field, and `Bill Bell` in the **Pronounceable name** field, the speech engine recognizes both William Bell and Bill Bell.

Each site has a default language setting. You must specify the user name using the language associated with the user site. If an Auto Attendant includes other sites that have different default languages, the callers at Auto Attendant will have to say the names in the language specified to look up a user.

For example, Site 1 has the default site language set to US English. Additionally, Site 1 Auto Attendant includes Site 2 where the default site language is set to Canadian French. The caller has to use French to look up a user in Site 2 or use English to look up a user in Site 1.

Hence, when including other sites in the same Auto Attendant, Avaya recommends that you must ensure that all sites have the same default site language to ensure optimal recognition accuracy and efficiency.

User Management field descriptions

Name	Description
License Status	
License mode	The license modes include: • Normal • Restricted • Error
Edit User / Info Mailbox	
Identifier	The mailbox number for the user whose properties you want to edit.
Add User/Info Mailbox	

Name	Description
Add a new user	The **Add** button opens the User Management > Properties for the New User Web page.
Add a new Info Mailbox	The **Add** button opens the User Management > Properties for the New Info Mailbox Web page.
Add User by AD lookup	This section is only available if you configure the Exchange storage destination.
AD search	To perform an Active Directory search, the Messaging system provides the Active Directory field name drop-down list, comparator drop-down list, and a text field for you to enter data. You can perform an Active Directory search using any of the following: • mail • telephone number • name

User Management > Properties field descriptions

Name	Description
User Properties	
First name	The first name of the user.
Last name	The last name of the user.
Display name	The name that Messaging displays during communications.
ASCII name	The ASCII name of the user.
Storage destination	The storage destination for your messages. The options are: • **Avaya Message Store** • **Microsoft Exchange**
Exchange Properties	
Exchange email address	The Exchange email address.

Name	Description
	The system does not display the field if the current message storage destination is **Avaya Message Store**.
Exchange server FQDN	The FQDN for Microsoft Exchange. The system does not display the field if the current message storage destination is **Avaya Message Store**. If you select the **Use Autodiscover service** check box on the Storage Destinations Web page, you cannot edit the field. After you click **Save**, the system populates the field.
Site	The name of the site on which the user is a member. For more information about sites, see Setting site properties for the first time on page 83.
Mailbox number	The mailbox number of the user. All mailbox numbers must be unique.
Internal Identifier	The internal identifier of the user. The system displays this field only if you are editing an existing user.
Numeric address	The unique identifier for the user. The system displays this field only if you are editing an existing user.
Extension	The telephone extension of the user. The extension length must match the site length. For more information, see Sites field descriptions on page 89. Usually, the extension is unique. However, if you share the extension with another user, Messaging displays the name of both the users and prompts callers to select the desired mailbox.
Include in Auto Attendant directory	The Messaging system adds the user to the Auto Attendant directory. See Sites field descriptions on page 89.
Additional extensions	The additional extensions roll over to the same voice-messaging mailbox. You define additional extensions when a mailbox migrates from a legacy phone system. For example, when you must maintain both the old and the new extension in the internal directory.
Class of Service	The CoS of the user. Select the CoS from the drop-down list. The CoS controls user access to features and provides general settings such as mailbox size.

Name	Description
	For more information, see Class of Service overview on page 155.
Pronounceable name	The pronounceable name of a user. The name of a user, info mailbox, or distribution list might not follow the pronunciation rules of the primary language for your system. To increase the likelihood of the Speech Recognition feature recognizing the name, spell the name, as you would pronounce the name. For example, if the primary language of your system is English, spell Dan DuBois as `Dan Doobwah`. You can also enter an alternative name for the user. For example, William Bell might also be known as Bill Bell. If you enter `William` in the **First name** field, `Bell` in the **Last name** field, and `Bill Bell` in the **Pronounceable name** field, the speech engine recognizes both William Bell and Bill Bell.
MWI enabled	The field to enable the message waiting indicator (MWI) light feature. The options are: • *Yes:* When the user has a deskphone • *No*: When the user has a voice mailbox only • *ByCOS:* When the CoS controls how the system enables MWI The **MWI enabled** field overrules the MWI setting defined by the CoS to which the user is associated.
Miscellaneous 1	The additional information about the user. The value in the **Miscellaneous 1** field in the Messaging system is found only on the SMI page and nowhere else.
Miscellaneous 2	The additional information about the user. The value in the **Miscellaneous 2** field in the Messaging system is found only on the SMI page and nowhere else.
New password	The password the user must use to log in to the Messaging mailbox. Passwords cannot match the voice mailbox number, cannot be sequential numbers, and cannot contain the mailbox number. If you do not enter a value for an existing user, the system does not change the existing password.
Confirm password	The password that the user must enter to confirm the value in the **New Password** field.

Name	Description
	Enter a password only if you are adding a new password or changing an existing password.
User must change voice messaging password at next logon	The check box to enable the user to change the password the next time the users call in to the voice mailboxes. By default, Messaging requires that new users change the temporary passwords when the users log in to the mailbox for the first time.
Voice messaging password expired	The check box to enable the user to continue using the password even after the password has expired. If a user password expires, Messaging enables the check box. Clear the check box to allow the user to continue using the expired password.
Locked out from voice messaging	The check box to prevent the user from accessing the Messaging system. Messaging automatically locks the system when the user fails to enter proper login credentials after a certain number of consecutive failed attempts. The **Lock out users after** field on the System Policies Web page determines the number of consecutive failed attempts that the system allows. Clear the check box to provide the user access to the system.
Advanced Tasks	
Reset the message waiting indicator for extension	The option to reset Message Waiting Indicator (MWI) for the user extension. For an Exchange user, use **Reset** to: • Rediscover the EWS server if you have selected the **Use Autodiscover service** check box on the Storage Destinations Web page. • Resubscribe to push subscriptions. • Reset MWI if you have enabled MWI for that user. For an Avaya message store user, clicking **Reset** only resets MWI.
User Preferences	
Open User Preferences	The link to open the User Preferences Web page for the user whose details you are viewing.

Comments? infodev@avaya.com

Configuring system policies

Use the System Policies Web page to configure advanced settings for the Messaging system.

Procedure

1. Use a privileged user account and password to log in to the server that is running the storage role.
2. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Policies**.
3. On the System Policies Web page, enter the appropriate information.
   For more information, see System Policies field descriptions on page 143.
4. Click **Save**.
   The system saves the details.

System Policies field descriptions

Name	Description
Password Policy	
Minimum password length	The minimum number of characters required for a password. The default is *4*. The range is *3* to *15*.
Maximum password length	The maximum number of characters required for a password. The default is *15*. The range is *3* to *15*.
User passwords expire	The number of days after which the password expires. The default is *0*. The range is *0* to *999*.
Warn users	The number of days before the current password expires and the day the system starts sending the user a warning to change the password. The default is *0*. The range is *0* to *999*.

Name	Description
Lock out users after	The number of failed login attempts before the system locks the user account. The default is *9*. The range is *0* to *99*.
Caller Applications Administrator	
Password	The password for accessing Caller Applications Editor.
Confirm password	Confirm the password for accessing Caller Applications Editor.
Private Messages	
Allow email notification for private messages	This setting is relevant if you have enabled the email notification in the CoS for one or more users. The system allows you to send private messages as email notifications to the user mailbox. The options are: • Yes, with or without recording • Yes, only without recording • No If allowed, users receive email notifications depending on the Notify Me settings within their personal User Preferences. The system delivers email notifications in the .wav file format.

The following table describes the various combinations for a user to receive a private message email notification:

System Policies - Allow email notification for private messages	User Preferences: Notify Me - Email Notifications	Result
Yes, with or without recording	E-mail me a notification for each voice message	User receives email notification without the recording.
Yes, with or without recording	E-mail me a notification for each voice message and include the recording	User receives email notification with or without the recording.
Yes, only without recording	E-mail me a notification for each voice message	User receives email notification without the recording.

System Policies - Allow email notification for private messages	User Preferences: Notify Me - Email Notifications	Result
Yes, only without recording	E-mail me a notification for each voice message and include the recording	User receives email notification without the recording.
No	E-mail me a notification for each voice message	User does not receive email notification.
No	E-mail me a notification for each voice message and include the recording	User does not receive email notification.

Manage info mailboxes

Info mailbox overview

An info mailbox plays greetings and provides information to a caller. However, a caller cannot leave a message in the info mailbox. Examples of the content of an info mailbox include:

- Directions to your location.
- Your business hours.
- Weather or road conditions.
- School enrollment or closing announcements.
- Human resources announcements.
- The name of the info mailbox in the Auto Attendant directory is a Text-to-Speech playback of the display name.
- *Info Mailbox* is the default name of the CoS that controls the maximum length of a recorded message in an info mailbox.
- The default value for the maximum length of a message in an info mailbox is 5 minutes. You can change the default value on the Class of Service Web page. See Changing a Class of Service on page 156.

Adding an info mailbox

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. In the **Add a new Info Mailbox** area, click **Add**.
3. Enter the appropriate information in the fields.

   For more information, see Properties for New Info Mailbox field descriptions on page 146.
4. Click **Save**.

   The info mailbox does not require a seat license.

   The system adds the info mailbox.

Next steps

Use your TUI to record the voice message for the info mailbox.

Properties for New Info Mailbox field descriptions

Name	Description
First name	The first name of the info mailbox.
Last name	The last name of the info mailbox.
Display name	The display name of the info mailbox that Messaging displays during communications.
Site	The name of the site of which the info mailbox is a member. For more information about sites, see Setting site properties for the first time on page 83.
Mailbox number	The mailbox number of the info mailbox. All mailbox numbers must be unique.
Internal Identifier	The email address of the info mailbox. The system displays this field only if you are editing an existing user.
Numeric Address	The unique identifier of the info mailbox. The system displays this field only if you are editing an existing user.

Name	Description
Extension	The telephone extension of the info mailbox. The extension length must match the site length. For more information, see Sites field descriptions on page 89.
Include in Auto Attendant directory	Adds the mailbox to the Auto Attendant directory. See Sites field descriptions on page 89.
Additional Extensions	Additional extensions that roll over to the same voice messaging mailbox. Additional extensions are often defined when a mailbox migrates from a legacy phone system, for example, when both the old and the new extensions need to be maintained in the internal directory.
Class of Service	The CoS of the info mailbox, usually *Info Mailbox*. The CoS controls user access to features and provides general settings such as mailbox size. For more information, see Class of Service overview on page 155.
Pronounceable name	The name of an info mailbox might not follow the pronunciation rules of the primary language for your system. To increase the likelihood of the Speech Recognition feature recognizing the name, spell the name, as you would pronounce the name. For example, if the primary language of your system is English, spell Dan DuBois as `Dan Doobwah`. You can also enter an alternative name for the mailbox. For example, if you enter `Hours` in the **Last name** field, and `Business hours` in the **Pronounceable name** field, the speech engine recognizes both names.
After the Greeting Plays	The action Messaging takes after playing the greeting. The options are: • *Hang up* • *Transfer to* the mailbox number that you enter
New password	The password the user must use to log in to the Messaging mailbox.

Name	Description
	If you do not enter a value for an existing info mailbox, the system does not change the existing password.
Confirm password	Confirmation of the value in the **New Password** field. Enter a password only if you are adding a new password or changing an existing password.
User must change voice messaging password at next logon	To force users to change passwords the next time the users call in to their info mailboxes. By default, Messaging requires that new users change the temporary passwords when the users log in to the mailbox for the first time.
Voice messaging password expired	To allow the user to continue using the user password that has expired. If a user password expires, Messaging enables the check box. Clear the check box to allow the user to continue using the expired password.
Locked out from voice messaging	Prevent user access to the Messaging system. Messaging automatically locks the system when the user fails to enter proper login credentials after a certain number of consecutive failed attempts. The **Lock out users after** field on the System Policies Web page determines the number of allowable consecutive failed attempts. Clear the check box to provide the user access to the system.

Manage mailboxes

Adding a mailbox

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.

Comments? infodev@avaya.com

2. In the **Add a new user** area on the User Management Web page, click **Add**.
3. Enter the appropriate information in the fields.
4. Click **Save**.
5. Repeat Step 2 through Step 4 for each additional user mailbox that you want to add.
6. Notify the new users that the Messaging service is available.

Deleting a mailbox

Procedure

1. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.
2. Use the built-in filters to locate the user mailbox that you want to delete and then click the appropriate **Mailbox** number.

   You can also delete the user mailbox from the User Management Web page. However, the User Management Web page does not have filters that assist you in locating a specific user.
3. On the User Management > Properties Web page, click **Delete**.
4. In the confirmation screen, click **OK** to continue.
   The system deletes the mailbox.

Unlocking the voice mailbox account

Use the following procedure to unlock the voice mailbox account of a user.

Procedure

1. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.
2. Use the built-in filters to locate the user mailbox that you want to update and then click the appropriate **Mailbox** number.

   You can also change the user properties from the User Management Web page. However, the User Management Web page does not have filters that assist you in locating a specific user.
3. On the User Management > Properties Web page, clear the **Locked out from voice messaging** check box.

   By clearing the **Locked out from voice messaging** check box, the user can use the correct login credentials to log in to the voice mailbox at the next logon.

Messaging automatically locks the system when the user fails to enter proper login credentials after a certain number of consecutive failed attempts.

Using the **Lock out users after** field on the System Policies Web page, you can set the number of consecutive failed attempts for the system.

4. Click **Save**.
   The system saves the settings.

Resetting the voice mailbox password

Use the following procedure to reset the voice mailbox password of a user.

Procedure

1. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.
2. Use the built-in filters to locate the user mailbox that you want to update and then click the appropriate **Mailbox** number.

   You can also change the user properties from the User Management Web page. However, the User Management Web page does not have filters that assist you in locating a specific user.
3. On the User Management > Properties Web page, in the **New password** field, enter a password that the user must use to log in to the Messaging mailbox.

   Passwords must not match the voice mailbox number, cannot be sequential numbers, and cannot contain the mailbox number. If you do not enter a value for an existing user, the system does not change the existing password.
4. In the **Confirm password** field, re-enter the password that you entered in the **New password** field.

   You must complete this field only if you are adding a new password or changing an existing password.
5. Click **Save**.
   The system saves the settings.

Changing the voice mailbox password

Use the following procedure to enable a user to change the voice mailbox password at the next logon.

Procedure

1. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.
2. Use the built-in filters to locate the user mailbox that you want to update and then click the appropriate **Mailbox** number.

   You can also change the user properties from the User Management Web page. However, the User Management Web page does not have filters that assist you in locating a specific user.
3. On the User Management > Properties Web page, select the **User must change voice messaging password at next logon** check box.

   By selecting the check box, you force the user to change the voice mailbox password at next logon. By default, Messaging requires that new users change the temporary password when the users log in to the voice mailbox for the first time.
4. Click **Save**.
   The system saves the settings.

Manage remote users

Types of remote users

Your voice mail network can include the following types of remote users:

- Administered remote users: Users defined as remote users within the local system. You must define remote users when you:
  - Conduct remote updates. For more information, see Remote updates on page 152.
  - Manually administer a remote user instead of waiting for a remote update. For more information, see Running a remote update manually on page 153.
- Unverified remote users: Remote users are unknown to the local system. Unverified remote users automatically become verified non-administered remote users when the system goes through the remote update process.
- Verified non-administered remote users: Remote users are present in the local database only because these users have successfully exchanged messages with the local system.

Addressing remote users

You can address remote users using the numeric address, dial by name, or speech addressing feature.

Remote updates

Remote updates provide an automatic method of administering remote users. Using remote updates:

- You can automatically add all remote users who need to exchange messages across the network.
- Your local Messaging system can exchange user information with each remote Messaging system that you have administered on the local system.

Remote updates greatly reduce the time required to set up the Messaging digital network. Using the remote updates feature depends on:

- The number of users in your network.
- The size and disk space of your local system.
- The number of networking ports that you are using.

You also can manually enter remote user information. Before you administer your user or remotely 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

Complete updates exchange all user information between all systems. When you add a new system 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, you must perform complete updates during non-prime time to reduce the impact on system users.

Additionally, the local Messaging system can automatically schedule a complete update during non-prime 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 you add a new user to a remote system or a local system.

When all systems in the network allow remote updates, the system whose database of users has changed notifies each system in the network.

Setting up remote updates

Complete this procedure on each Messaging server in your local system.

Before you begin

- The administrator for each remote system has agreed to allow remote updates from your local system.
- Your local server connects to at least one remote server. See Adding a network server on page 113.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Storage)** > **Networked Servers**.
   If you already have servers networked to your local Messaging system, the Manage Networked Servers Web page displays the details of each server.
2. Select the server that you want to enable for remote updates.
3. Click **Edit the Selected Networked Server**.
4. Enable the **Updates In** and **Updates Out** fields.
5. Click **Save**.
   The system modifies the server information successfully.
6. Repeat the procedure on each networked server from which you want to receive remote updates.

Running a remote update manually

About this task

If you need to quickly populate the user database or correct database inconsistencies that the system discovered during an audit, you must manually run a remote update.

Note:

Avoid running the remote update during prime time hours. Depending on the number of users on the remote system, the remote update may take hours to complete.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Reports** > **Measurements (Storage)**.

2. On the Messaging Measurements Web page, select *Feature* from the **Type** drop-down list.
3. Set the **Cycle** to *Daily*.
4. Click **Get Report**.
5. Note the current number of remote users.
6. On the **Administration** menu, click **Messaging** > **Server Settings (Storage)** > **Request Remote Update**.
7. On the Request Remote Update Web page, select a server from the drop-down list.
8. Click **Request Update**.

   Tip:

   Click **Refresh Update Status** to verify the status of the update.
9. Return to the Messaging Measurements Web page and confirm the number of remote users.
10. Repeat Step 2 through Step 5.
11. On the **Administration** menu, click **Messaging** > **Logs** > **Administrator**.
12. On the Administrator's Log Web page, click **Display** and verify that no conflicts or problems occurred with the remote update.

Request Remote Update field descriptions

Name	Description
Request Update	Request a remote update of user data.

Comments? infodev@avaya.com

Chapter 9: Class of Service

Class of Service overview

A CoS defines the privileges and the features assigned to a group of users.

- Use the Class of Service Web page to define each CoS, create new CoSs, and change or rename existing CoSs. You can create a maximum of 512 CoSs. The maximum storage size for a CoS is 65536 KB.
- Use the User Management Web page to assign a previously defined CoS to a user.

Default Classes of Service:

Messaging comes with the following default CoSs that you can assign to each user:

- *Standard* or *Enhanced*: To allow local and domestic long-distance dialing.
- *Executive*: To allow local, domestic long-distance, and international dialing.
- *Info Mailbox*: To create a message for an info mailbox. A typical informational message might include details about directions, business hours, weather, or human resources information. You can record messages for an info mailbox that take up to 5 minutes to play.

  To create an info mailbox, follow the instructions for Adding an info mailbox on page 146. You cannot create an info mailbox by assigning the Info Mailbox CoS to the user.

  An info mailbox does not require a seat license.
- *Administrator* allows you to send system broadcast messages. A typical system broadcast message includes announcements or instructions from the system administrator about the voice mail system. This CoS is unrelated to the administrative privileges handled through the Server (Maintenance) RBAC administration. Messaging supports two levels of broadcast messages.
  - System level: Subscribers with system level broadcast recording privilege can record system level broadcast messages. The system level broadcast message goes to all subscribers who belong to the sites managed by the application server.
  - Site level: Subscribers with site level broadcast recording privilege can record site level broadcast messages. The site level broadcast message is restricted to only the subscribers who share the same site as the recording subscriber.

Note:

Site level broadcast message recording is only supported in the Aria TUI.

- ELA allows you to use the Enhanced-List Application.

For more information, see Class of Service field descriptions on page 158.

Adding a Class of Service

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. On the Class of Service Web page, click **Add New**.
3. Enter the appropriate information in the Class of Service Web page.
   For more information, see Class of Service field descriptions on page 158.
4. Click **Save**.
   The system saves the details.

Changing a Class of Service

The CoS control of a feature only extends to controlling access to the GUI or TUI where the user manages the feature. If a user had the feature enabled previously, the CoS does not *switch off* the feature.

The following features are actively enabled by users, and will therefore keep on functioning even if you change the CoS definition of a user to disallow the use of the enabled feature any more:

- Reach Me
- Notify Me

You must disable the above features using the User Preferences Web pages prior to disabling the features from the CoS.

Note:

If you use the CoS to disable the above features prior to disabling from the User Preferences Web pages, the user can no longer change the settings for these features. However, if you enabled the feature previously, the user can continue to use the feature. Hence, you must

ensure that the users are no longer using the features that are to be deleted from their CoS, prior to implementing this change.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. Select the CoS that you want to change from the **Class of Service** drop-down list.
3. Make your changes.
   For information about the fields on this page, see Class of Service field descriptions on page 158.
4. Click **Save**.
   The system saves the changes.

Deleting a Class of Service

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. Select the CoS that you want to delete from the **Class of Service** drop-down list.
3. Click **Delete**.
   The system displays a confirmation dialog.
4. Click **OK** to proceed.
   The system deletes the CoS.

Basic and Mainstream mailbox licensing

Messaging offers mailbox licenses for Basic and Mainstream users.

- Basic: Provides the basic call answering and voice messaging functionality.
- Mainstream: Provides the full functionality of the Messaging system that includes call answering, voice messaging, Reach Me, Notify Me, fax support, speech based features, and IMAP access to the Avaya message store.

Administrators can mix the Basic and Mainstream seat licenses on the Messaging system.

Messaging offers a cost effective licensing model as customers who want only the Basic messaging features can purchase lower cost Basic mailbox licenses. Customers who want advanced capabilities can purchase the Mainstream mailbox licenses.

License status

The License Status Web page displays the type of license mode used in the Messaging system and error information. The Web page also displays the status of the license as enabled or disabled.

License modes include:

- *Normal*: The system also displays the license name, the number of users who have acquired a license, and the number of licenses your organization has purchased.
- *Restricted*: The system also displays information about the restriction.
- *Error*: The system indicates that you are in the grace period for new licenses.

The Messaging system provides a grace period of 30 days after the license expires. In the grace period, the License Status Web page displays a warning message. After the grace period, the system disables all user management activities except deleting users and all User Preferences changes. The only exception is that users can still change the password. This is to allow users to recover from lockout situations.

To view the License Status Web page, on the **Administration** menu, click **Licensing** > **Licensing** > **License Status**.

Class of Service field descriptions

Name	Description
Class of Service	The name of the CoS.

General:

Name	Description
Name	A customized name for the CoS. A descriptive name is more helpful than a number.
ID	The unique identification number for the CoS.

Comments? infodev@avaya.com

Name	Description
Required seat license	The type of seat licensing required for users who are members of this CoS. The options are: • Basic (VALUE_MSG_SEAT_BASIC) • Mainstream (VALUE_MSG_SEAT_MAINSTREAM) The system does not display this field for a new CoS. For more information on the types of licensing, see Basic and Mainstream mailbox licensing on page 157. The section at the end of this table lists the features that require a mainstream license.
Telephone User Interface	The TUI for users assigned to this CoS. The options are: • Aria • AUDIX The default is *Aria*.
User can send to system distribution lists (ELAs)	To allow the user to send messages through Enhanced-List Application (ELA) distribution lists. For more information about ELAs, see Enhanced-List Application overview on page 169.
Fax support	Enables fax receiving for users assigned the CoS using the fax receiving method configured on the application servers for the sites belonging to the user. The selected fax support method must match the fax receiving method configured on the application servers for the sites belonging to the user to ensure that Messaging displays the correct fax options in User Preferences. For more information, see the configuration of the **Fax receiving** field in System Parameters field descriptions on page 125. If you have not configured fax support at the CoS level, Messaging refuses fax transmissions intended for users in that CoS.
Dial-out privilege	The types of calls that the system allows users in this class to make when using the Call Sender, Play on Phone, Reach Me and Notify Me features. Possible values are

Name	Description
	None, On Premise, Local, Long Distance, and International.
User can use Reach Me	The user can use the *Reach Me* feature. For a new CoS, the system selects this check box by default. If you clear the check box, the system does not allow the user to update the Reach Me page in User Preferences. If you change the value in the **Dial-out privilege** field to: • None, the system clears and disables this check box. • anything else other than *None*, the system enables and selects this check box.
Allow voice recognition for addressing (user can select recipients by saying their name)	The user can select recipients by saying their name. For a new CoS, the system selects this check box by default. If you clear the check box, the system does not allow the user to update the Voice Recognition for Addressing area in the My Phone page in User Preferences.
IMAP/POP3 access	Indicates the use of an IMAP/POP3 client to access the messages stores on an Avaya message store. The options are: • None • Full: You can use an IMAP4/POP3 client to access the messages stored on an Avaya message store. The default is *Full*.
Set Message Waiting Indicator (MWI) on user's desk phone	For users with an MWI lamp on their deskphone, the lamp lights up when an unheard message is in the inbox.
Enable password aging	Indicates whether users must periodically change their passwords. If users do not change the user passwords within a specified time, the passwords expire and Messaging blocks the user until an administrator resets the passwords. The default is to disable password aging. You can:

Name	Description
	• Set the aging parameters on the System Policies Web page. See Configuring system policies on page 143. • Reset expired passwords by clearing the **Voice messaging password expired** field on the User Management > Properties Web page. See Changing user properties on page 136.
Broadcast message recording	Indicates whether a user can send system broadcast messages. The options are: • None • Allow system level broadcast message recording: Subscribers with system level broadcast recording privilege can record system level broadcast messages. • Allow site level broadcast message recording: Subscribers with site level broadcast recording privilege can record site level broadcast messages. This option is visible only when you have selected Aria TUI from the **Telephone User Interface** drop-down. **Note:** Site level broadcast message recording is only supported in the Aria TUI. For broadcast messages, the MWI on the deskphone of the user does not light up.

Greetings:

The Greetings fields control the number, type, and length of greetings that each user can record.

Name	Description
Normal greetings a user can record	The number of greetings a user can record. The options are: • None • Personal internal and external greetings • Personal and optional greetings
Maximum length	The maximum length of a greeting in seconds.

Name	Description
	The range is 5 to 300 seconds for personal and optional greetings. The range is 5 to 90 seconds for extended absence greeting.
User can record extended absence greeting	Specifies whether users can record an Extended Absence Greeting (EAG). Callers cannot dial-through an EAG. The system allows fax transmission even if a user has EAG enabled.
Block message recording if extended absence greeting is recorded	The system blocks callers from leaving a message if the user has activated EAG.

Notifications:

Using the Notifications fields, the users can gain access to the notification features. The system displays each notification feature that you enable on the Class of Service Web page on the Notify Me Web page in User Preferences. The system hides features that you do not enable.

After you complete the information on the Class of Service Web page, individual users can gain access to User Preferences, enter their personal information on the General and Notify Me Web pages, and begin using the Notify Me features that you enabled.

Name	Description
Allow text message (or page) notification	The system sends a text notification to a mobile phone or pager to notify the user that the system delivered a new voice message to the user mailbox. If allowed: • The administrator must provide the email address for the appropriate SMS gateway. See Adding mobile operators on page 165. • Users must enable the Notify Me settings within their personal User Preferences. Messaging supports only email based (SMTP) pager and cellular notifications.
Allow outcalling notification	Enables outcalling. Outcalling alerts a user to new messages by having the system place a call to that user. Outcalling requires that users have the appropriate dial-out privileges.
Maximum number of rings	The maximum number of times the phone that the user has designated as the outcall

Name	Description
	phone rings before the system hangs up during an outcall attempt. The range is 1 to 10. This field is disabled if **Allow outcalling notification** is No.
Start after	The length of the delay between the time a user receives a message and the first outcall attempt. The range is 0 minutes to 24 hours.
If no-answer or busy, retry after	The length of the delay between an unsuccessful outcall attempt and a new outcall attempt. The called phone can be unanswered or busy. The range is 5 minutes to 24 hours.
Stop after	The length of the delay between the time the user received the message and the system ends the outcall attempts. The range is 0 minutes to 24 hours.
Allow email notification	The Messaging system sends a text message to an email address to notify the user that the system delivered a new voice message to the user mailbox. The options are: • Yes, with or without recording • Yes, only without recording • No If allowed, users must *also* enable the Notify Me settings in User Preferences. The system delivers email notifications in the .wav file format.

Message Storage:

Using the Message Storage fields, you can control the amount of space that a user has on the message store.

Name	Description
Maximum storage space	The maximum storage space allocated to an individual user. The range is 0 to 65536 KB. The default is *65536* KB.
Maximum call answer message length	The maximum duration of call answer messages a user can receive. The range is 64 to 46880 KB.

Name	Description
	The default is *2400* KB.

Message Retention:

Using the Message Retention fields, you can control the amount of time the system stores messages for the user.

Name	Description
Unread messages in Inbox folder	The numbers of days the unread messages are stored in the Inbox folder. The options are: • Keep messages forever. • Delete messages after the specified number of days. By default, the Messaging system deletes the messages after *45* days. The range is 0 to 999.
Read messages in Inbox folder	The numbers of days the read messages are stored in the Inbox folder. The options are: • Keep messages forever. • Delete messages after the specified number of days. By default, the Messaging system deletes the messages after *45* days. The range is 0 to 999.
Messages in other folders	Users with IMAP access to mailbox can create folders in addition to their Inbox folder. This setting controls the number of days messages are stored in a folder that the user creates. The options are: • Keep messages forever. • Delete messages after the specified number of days. By default, the Messaging system deletes the messages after *45* days. The range is 0 to 999.

The mainstream license is required for only the following features:

- Reach Me
- Notify Me
  - Text message or page notification

- Phone call to a telephone or mobile phone
- Email copy

• Fax

- Detect and transfer to fax server
- Receive and forward to email

• IMAP access to Avaya message store

• Speech based features

- Speech recognition for addressing
- Basic Speech Auto Attendant
- Access to Avaya one-X® Speech

All other Messaging features are available without requiring a mainstream license.

Adding mobile operators

If you allow users to receive text messages or pages on a mobile device, you must provide the address of the mail gateway for each mobile operator that your users might have.

The website for each mobile operator usually provides information about the mail gateway. Other websites provide a worldwide list of mobile operators that contains this information. Avaya does not guarantee the accuracy or completeness of the information on these websites. You must verify the information.

Note:

Some mobile operators only provide this functionality as a part of a premium service package.

Before you begin

Obtain the address of the mail gateway for each mobile operator that you plan to support.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. In the **Notifications** area of the Class of Service Web page, set the **Allow text message (or page) notification** field to *Yes*.

   Messaging supports only email based (SMTP) pager and cellular notifications.
3. Click the **Mobile Operators** link.

4. Enter the appropriate information in the **Mobile Operators Definitions for Text Message Notifications** area.

   For more information, see Mobile Operators field descriptions on page 167.

5. Click **Save**.
   The system saves the mobile definitions.

Next steps

Test the mail gateway for each mobile operator that you plan to support. See Testing mail gateways on page 166.

Testing mail gateways

Before you begin

- Complete the instructions for Adding mobile operators on page 165.
- Provide a test phone or pager for each mobile operator that you add to the Mobile Operators Web page. Messaging supports only email based (SMTP) pager and cellular notifications.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. In the **Notifications** area of the Class of Service Web page, click the **Mobile Operators** link.
3. Ensure that the email gateway address for the mobile operator that you want to test is present in the **Mobile Operator Definitions for Text Message Notifications** area. If the email gateway address is not present, see Adding mobile operators on page 165.
4. In the **Test** area, enter the appropriate information in the fields.

   For more information, see Mobile Operators field descriptions on page 167.

5. Click **Send**.
6. Validate that the mobile device received the test message.

Mobile Operators field descriptions

Name	Description
Internal ID	A unique identifier that describes the mobile operator. The name is internal to your organization and is *invisible* to users.
Description	The name of the operator that is *visible* to users.
Address template	The part of the email address that the operator uses that is the same for all users. The system substitutes *{0}* with the number for the user. The system uses the number from the Mobile phone or page field on the General Web page of User Preferences. If you need to add a prefix, put the prefix in front of the {0} variable.
Mobile phone (or pager) number	The phone or pager number of the test device. Messaging supports only email based (SMTP) pager and cellular notifications.
Mobile operator	The name of the mobile operator for the email address you want to test. The drop-down list displays the name that is present in the **Description** field.
Message	The text you want to send to your test device.

Deleting broadcast messages

If you select the **Allow system level broadcast message recording** or **Allow site level broadcast message recording** from the **Broadcast message recording** drop-down list on the Class of Service Web page, users can send broadcast messages using the TUI.

You can delete the broadcast message by logging in to the Aria TUI.

Note:

You cannot delete the broadcast message using the Audix TUI.

Procedure

1. Log in to the TUI.
   You will hear the following system prompt as part of the prompt for the mailbox main menu for en-US language: `For broadcast message, press 9.`
2. Press **9**.
   If there is a broadcast message, you will hear the following system prompt: `To review the broadcast message, press 1. To record a message, press 2. To erase the broadcast message, press 3.`

   If there is no broadcast message, you will hear the following system prompt: `There is currently no broadcast message. To record a message, press 2.`
3. To delete the broadcast message, press **3**.

Chapter 10: Distribution lists

Enhanced-List Application overview

You can use the Enhanced-List Application (ELA) to create distribution lists for delivering messages to a large number of recipients.

Messaging supports a maximum of 1,000 ELA lists. Each ELA list can have a maximum of 1,500 members. You can nest ELA lists to create larger lists.

Implementation prerequisites

Before you implement ELA, obtain the following information:

- An available CoS number. The default for ELA is 8. ELA uses the CoS number for list mailboxes and the shadow mailbox.
- A range of extensions to use for list mailboxes. You do not need this information to set up ELA. However, you need this information to provide extensions for the list mailboxes when you begin creating lists.

Implementing ELA

Procedure

1. Create and configure a shadow mailbox.
2. Configure ELA.
3. Create enhanced lists.
4. Add members to enhanced lists.
5. Test the enhanced list setup.

Creating a shadow mailbox

ELA distributes messages through a shadow mailbox. Use a configured shadow mailbox to block recipients from replying to ELA senders or distribution lists.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. In the **Add a new user** area, click **Add**.
3. Leave the **First name** field blank.
4. Enter a descriptive name in the **Last name** field.
   For example, `shadow_do_not_reply`.
5. Enter a **Mailbox number**.
6. Enter an **Extension**.
   The extension must match the entry in the **Mailbox number** field.
7. Enter a password in the **New password** field.
8. Confirm the password in the **Confirm password** field.
9. Click **Save**.
   For more information on the fields, see User Management Properties field descriptions on page 139.

Next steps

Configure the shadow mailbox on the System Mailboxes Web page.

Configuring a shadow mailbox

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Mailboxes**.
2. Enter the appropriate information required to configure a shadow mailbox.
   For more information, see System Mailboxes field descriptions on page 171.
3. Click **Save**.
   The system saves the configuration.

System Mailboxes field descriptions

Use the System Mailboxes Web page to make system-wide settings that apply to all users.

Name	Description
SYSTEM MAILBOXES	
Internet Postmaster Mailbox Number	The postmaster is responsible for managing the emails for a site. The postmaster mailbox is a system-wide mailbox set aside for the postmaster and is integral to the operation of the Messaging system.
Enhanced-List Application Shadow Mailbox Number	The mailbox number for the ELA shadow mailbox. Messaging uses the shadow mailbox and the Community ID settings to control the sending privileges of users who address messages to ELA lists.
SYSTEM ATTRIBUTES	
Maximum Administered Remotes	The maximum number of remote users that Messaging accommodates. The maximum value that you can enter is 250000.
Maximum Message Length	The number of minutes or megabytes of the longest message that a user can create. You can set additional restrictions for users on the Class of Service Web page.
Miscellaneous Field Names	
Miscellaneous 1 Field Name **Miscellaneous 2 Field Name** **Miscellaneous 3 Field Name** **Miscellaneous 4 Field Name**	Do not use these fields. Messaging will not support these fields in a future release.

Adding a new ELA list

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Enhanced List Management**.
2. On the Manage Enhanced-Lists Web page, click **Create a New List**.
3. Enter the appropriate information in the fields.

   For more information, see Create a New Enhanced-List field descriptions on page 173.
4. Click **Save**.
   The system saves the changes.

Next steps

- Reload the User List and Global Address List. For more information, see Loading lists on page 175.
- Configure the External Hosts and Mail Options with the **Alias** field blank. For more information, see Changing external SMTP hosts on page 131 and Configuring the mail options on page 307.

Manage Enhanced-Lists field descriptions

Name	Description
Server Name	The IP address of the server.
Number of Enhanced-Lists	The number of enhanced lists.
List Name	The name of each enhanced list.
Mailbox Number	The local mailbox number of each enhanced list.
Numeric Address	The unique identifying address of each enhanced list that users use to send messages to the ELA list.
Reply?	The system allows recipients of messages distributed by Enhanced-List Application to reply to list messages.

Name	Description
Bcast?	The system broadcasts messages sent to this list to all local users. To change the setting, select the list and then click **Change Attributes of Selected List**.
COS	The CoS assigned to each enhanced list.
CID	The Community ID of each enhanced list.

Create a New Enhanced-List field descriptions

Name	Description
BASIC INFORMATION *(Required Fields)	
***List Name**	The name of the list. The name can include up to 29 alphanumeric characters.
***Password**	The password for the Enhanced-List mailbox. The password must include numeric characters from 5 to 15. When you change an existing Enhanced-List, leave this field blank to retain the existing password. If you use an email client to log in to the Enhanced-List mailbox, you must enter this password. You must not enter this password to send messages to the list.
***Mailbox Number**	A 3 to 10-digit mailbox number. ELA automatically creates a mailbox with this mailbox number if a mailbox does not already exist. If a mailbox with the specified number already exists, ELA converts the existing mailbox into a list mailbox. The mailbox number must: • Be within the range of numbers assigned to your system. • Not be assigned to another local user. • Be a valid length on the local machine. On a multisite system, the user mailbox can be of any length between 2 to 50 digits. The system validates the user mailbox against the translation rules as set on the application server.
Numeric Address	The unique identifier that users provide to address messages within the voice mail network.

Name	Description
	The numeric address can contain the mailbox number. However, the length of the numeric address must be at least one digit different from the length of the mailbox number. For example, if a mailbox number 5671234 is in area code 222, the numeric address is 2225671234.
PBX Extension	The primary telephone extension of the user. The telephony server calls this number for an internal call. The PBX Extension can be the same as the Mailbox Number.
***Class Of Service (COS)**	The CoS for ELA is *8–ELA*.
***Community ID**	Do not change this field. The Community ID allows or denies voice mail among different communities.
Messaging Locale	The language of the Messaging system.
ENHANCED-LIST FEATURES	
Permit Reply to Sender?	Specifies whether the system allows recipients to send replies to the originator of a message from an Enhanced-List. The default is *yes*.
Broadcast to All Local Subscribers?	The only option, *off*, sends ELA messages only to the list members you specify on the Manage Enhanced-List Web page. The system sends all broadcast messages as priority messages. Unheard broadcast messages do not take up space in a recipient mailbox.
SUBSCRIBER DIRECTORY	
Email Handle	The email handle of the list. Messaging automatically populates this field when you add a new list. However, you can change the value in this field. Do not enter the machine name and domain into this field. The system automatically adds this information when a user sends or receives an email. The default is <*ListName*>. For example: *AcctDept* .
Telephone Number	The telephone number of the list in the same format as the system displays the number in address book listings, such as in email client applications. The entry does not have a specified format. However, you must format all entries consistently. The entry can be up to 32 characters long and can contain any combination of digits (0 to 9), periods (.), hyphens (-) the plus sign (+), and parentheses ( ).
Common Name	The common name of the list.

Name	Description
	Messaging automatically populates this field when you add a new list. However, you can change the value in this field. The system displays the Common Name in address book listings, such as for email client applications. The default entry is the same as the ListName.
ASCII Version of Name	If the list name is in the multibyte character format, type the ASCII translation of the list name.
SUBSCRIBER SECURITY	
Immediately Expire Password?	Allows you to forcibly expire the mailbox password if you have a security situation such as a change in mailbox ownership. The default is *no*.
Is Mailbox Locked?	A user might complain that the mailbox is inaccessible, that is, locked, possibly because of several unsuccessful attempts to log in. In such situations, you can add an extra layer of protection by selecting yes to lock the mailbox in case of unsuccessful login attempts and prevent access to the mailbox.
MISCELLANEOUS	
Miscellaneous1 **Miscellaneous2** **Miscellaneous3** **Miscellaneous4**	Do not use these fields. Messaging will not support these fields in a future release.

Loading lists

About this task

Use the System Operations Web page to load the following lists:

- User List
- Global Address List

Note:

After adding users, you must reload GAL or wait for the system nightly maintenance to view the users on the Remote Users Reports Web page.

Procedure

1. On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**.

2. In the **Reload Caches** area, click **Reload** to load the appropriate list.

Administering an ELA List

After you create an ELA distribution list, the system displays the list on the Managed Enhanced-List Web page.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Enhanced List Management**.
2. On the Manage Enhanced-Lists Web page, you can click on the respective buttons to:
   - Sort the lists.
   - Display a report of all the lists.
   - Create a new list. See Adding a new ELA list on page 172.
   - Select a list and then open the list to display, add, or delete list members. You can view the existing extensions and add new ones. You can add local users, remote users, and email addresses. If you type a last name that is common to more than one user, the system pops up a window so you can select the desired user.
   - Delete a list.
   - Select a list to change the properties.

   An ELA list can contain nested ELA lists.

Sort Enhanced-List field descriptions

Name	Description
Sort Keys	The order in which the Manage Enhanced-Lists Web page displays enhanced lists. • The **Primary** column determines the first sort key in ascending or descending order. • The **Secondary** column determines the second sort key, in case of a tie in the primary sort.
Sort Order	The order in which the system displays the lists: • *ascending* order (a to z, 0 to 9) • *descending* order (z to a, 9 to 0)
Name	The name of each enhanced list.
Mailbox Number	The mailbox number of each enhanced list.
Numeric Address	The unique address of each enhanced list.
Class Of Service	The CoS number of each enhanced list.
Community ID	The community to which the system assigns each enhanced list.

Report of Enhanced-Lists field descriptions

Name	Description
List Name	The name of each enhanced list. You can click the list name to open the list membership and manage the members.
Mailbox Number	The mailbox number of each enhanced list.
Numeric Address	The unique address of each enhanced list.
Reply?	Indicates whether recipients of messages that ELA distributes can reply to enhanced list messages.

Name	Description
Broadcast?	Indicates whether the system broadcasts the messages sent to the list to all local users.
COS	The CoS number of each enhanced list.
CID	The community to which the system assigns each enhanced list.

Managing enhanced-list members and administrators

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Enhanced List Management**.
2. Select the list and click **Open the Selected List**.
   The system displays the Enhanced-List Membership and Administrators page. This page operates in two modes that you can toggle between: members list and administrators list.

   When you open the list, by default the system displays the members list.

   - From the members list, you can administer members of the selected list. If you click **Administer Administrators** button the system displays the administrators list. Also, the system changes the **Administer Administrators** button to the **Administer Members** button.
   - From the administrator list, you can administer administrators of the selected list. If you click **Administer Members** button the system displays the members list. Also, the system changes the **Administer Members** button to the **Administer Administrators** button.
3. On the Enhanced-List Membership and Administrators page, from the members list, you can click the respective buttons to:
   - Add new members.
   - Sort members by the mailbox number or address.
   - Display a report of all members.
   - Open the nested ELA list.
   - Delete the selected member.
4. On the Enhanced-List Membership and Administrators page, from the administrators list, you can click the respective buttons to:
   - Add users to the list of administrators. Users who are assigned administrator roles in an ELA distribution list can see an Enhanced List page in User Preferences. These users can add or delete members from the ELA

distribution list. For more information, see *Chapter 3: Customizing Messaging* of *Using Avaya Aura® Messaging*.

- Sort administrators by the mailbox number or address.
- Display a report of all administrators.
- Delete the selected administrator.

Enhanced-List Membership and Administrators field descriptions

Table 1: Common fields

Name	Description
List Name	The name of the enhanced list.
Replies Permitted?	Indicates whether the system allows recipients of messages distributed by Enhanced-List Application to reply to list messages.
Broadcast?	Indicates whether the system broadcasts the messages sent to the list to all local users.
List Mailbox Number	The local mailbox number of the enhanced list.
Number of Members	The number of members in each list.
Number of Administrators	The number of administrators in each list.

Table 2: Manage members

Name	Description
Enter Address	The mailbox number or address of the member.
Add Member	Click to add a new member.
Member Name	The member name.
E-list?	Indicates whether the member belongs to the enhanced list.
Mailbox Number/Address	The mailbox number or address of the member.

Table 3: Manage administrators

Name	Description
Enter Address	The mailbox number or address of the administrator.
Add Administrator	Click to add a new administrator.
Administrator Name	The administrator name.
Mailbox Number/Address	The mailbox number or address of the administrator.

Enhanced-List Membership Report field descriptions

Field name	Description
List Name	The name of the enhanced list.
Replies Permitted	Indicates whether the system allows recipients of messages distributed by Enhanced-List Application to reply to list messages.
Broadcast	Indicates whether the system broadcasts the messages sent to the list to all local users.
List Mailbox Number	The local mailbox number of the enhanced list.
Number of Members	The number of members in each list.
Member Name	The member name.
E-List?	Indicates whether the member belongs to the enhanced list.
Mailbox Number	The mailbox number of the member.
Numeric Address	The numeric address of the member.
Email Address	The email address of the member.

Chapter 11: Caller applications

Caller applications overview

Caller applications enhance the TUI with custom menus and prompts that guide callers to the appropriate recipient. A caller application contains all custom menus and prompts associated with a unique mailbox.

When you create a caller application, you associate the caller application with a site. The storage server for that site deploys the caller application to each application server in the cluster. You can use the Microsoft Management Console (MMC) to import and export caller applications as XML data to other storage servers in a multisite environment.

Because Messaging stores each caller application as an LDAP Contact in a central mailbox, the system backs up caller applications each time you back up the message store.

Caller Applications Editor

Use Caller Applications Editor to create custom menus and to configure caller application properties. In the Messaging environment, caller applications perform the same functions as Automated Attendants. Caller Applications Editor runs as a plug-in within the MMC. You can gain access to information about MMC through the MMC Help menu.

System requirements

To use Caller Applications Editor, you need:

- A computer that is running one of the following operating systems:
  - Windows Server 2003
  - Windows Server 2008
  - Windows XP
  - Windows Vista
  - Windows 7
- The following software which is available from the Microsoft Download Center:
  - MMC 3.0

- .NET 3.5

- Administrative permissions on the computer.

Containers

Using a MMC container, you can group related items. MMC displays containers as folders in the navigation pane of Caller Application Editor. For more information about containers, see MMC Help.

Each caller application includes a container that stores parameters for the menu logic, prerecorded prompts, schedules, and other information. When you create a container, you map the container to a user account. Each caller application container includes the following properties.

- The name of the caller application.
- A unique mailbox number and extension for the caller application.
- Any additional extensions that you want to associate with the caller application.
- A flag for including the caller application in the Auto Attendant directory.
- An optional pronounceable name that supports the speech recognition feature of Auto Attendant.
- The time zone of the application server and not the storage server, if different.
- The caller menu logic.

For more information, see:

- Worksheet for container properties on page 189.
- New Caller Application field descriptions on page 196.

Prompts

You can use the following formats to create prompts that support the caller application menus:

- Prerecorded audio prompts in .wav format
- Text-to-Speech prompts

Recording an audio prompt

Procedure

1. Open the application that you use to record *.wav* files, such as Microsoft Sound Recorder.
2. Set the recording parameters according to your requirement.
3. Speak into a microphone that is connected to the computer and record the greeting.
4. Assign a name to the *.wav* file. Ensure that the resulting file name on the computer has the *.wav* file extension as part of the name.
5. Play the greeting on the computer before you transfer the file to the greetings source.

Changing the .wav file format

The .wav file requires the mu-law format, 8,000 kHz/8-bit mono. If you want to create an application prompt from a .wav file, the .wav file must use the same encoding, G.711 PCM mu-law, that all Caller Application prompts use. You must create an empty application prompt in the usual way.

If the encoding is correct, you must simply drag the .wav file into Voice Control of the Caller Applications Editor Prompt property page and save the file.

If the encoding is incorrect, you must use an application such as Microsoft Sound Recorder to create a file with the correct encoding.

Text-to-Speech prompts

You can enter a Text-to-Speech prompt as simple text. However, the following characters require additional encoding:

Unsupported characters	Encoded characters
<	<
>	>
&	&

Unsupported characters	Encoded characters
'	'
“	&quot

Menus

Caller application menus are based on dual-tone multi-frequency (DTMF) key entries that route calls to a unique mailbox. Use Caller Applications Editor to define menus that play during:

- Business hours
- Off hours
- Holidays

Menu components

Each menu includes:

- An *On Answer* welcome greeting that the caller hears when the system first answers a call.
- An *Instruction* prompt that defines the menu actions.
- Up to 10 DTMF key entries that act upon the menu actions defined by the Instruction prompt.

Menu flexibility

Caller Applications Editor guides you through the On Answer and Instruction prompts. However, you must create the logic for the DTMF key entries. Use the built-in flexibility of the key assignments to design custom menus that meet your specific needs. You must create the key presses and the key sequence.

A Business Hours menu has a set of prompts and DTMF key entries. An Off Hours menu is typically much simpler and can include only an On Answer prompt that explains that business is closed. However, Caller Applications Editor provides the same set of options and the same degree of flexibility for both types of menus.

Menu actions

When you create a menu, you must select the type of action that each key should perform. These actions are:

Action	Description

Comments? infodev@avaya.com

Auto Attendant	Forwards the call to the Auto Attendant so the caller can dial-by-name or dial-by-extension.
Go to mailbox number	Routes the call to a specified voice-messaging mailbox. For example, a non-business hours mailbox or an information-only mailbox.
Subscriber login	Routes the call to the voice messaging pilot extension so that users can log in to the personal mailbox.
Transfer to Caller Application	Transfers the call to an additional caller application.
Continue menu	Invokes the next action in the menu. For example, the Instructions prompt can use this as the *Next* action.
Hang up	Ends the call.
Transfer to extension	The system transfers the call to another extension. For example: • Transfer to a specified extension, such as Customer Service. • When a user forwards calls to a caller-application extension. For example, if an employee changes internal extensions or if a previously used extension is out of service.
Not active	The default for all DTMF keys before you assign an action. Unused keys must maintain this action. You cannot assign an action to the **On Answer** menu item.
Play prompt	Plays the specified audio file or text-to-speech prompt. After the system plays the prompt, the caller application starts the next action.

Example menu

The following table is an example of a Business Hours menu.

	Change action or select the prompt dialog	
Menu action	**First perform this action:**	**Then perform this action:**
On Answer	**Play prompt**	**Continue menu**

	Change action or select the prompt dialog	
Menu action	**First perform this action:**	**Then perform this action:**
	Use Text to Speech to say: *Hello, Welcome to the ABC store.*	Play the Instructions prompt.
Instructions	**Play prompt** Use Text to Speech to say: *Press 1 for business hours.* *Press 2 for directions to the store.* *Press 3 to dial an extension for the person you are trying to reach.* *Press 4 to spell the name of a person.* *Press 5 to leave a message.* *Press 6 to speak with an agent.* *Press 7 for all other inquiries.*	—
Key 1	**Play prompt** Use Text to Speech to say: *The ABC store is open from 10 a.m. to 7 p.m., Tuesday through Saturday.*	**Continue menu** The caller can press another key or hang up.
Key 2	**Play prompt** Use Text to Speech to say: *To get to the ABC store from downtown, take the number 1 bus and get off at Main Street. The ABC store is across the street.*	**Continue menu** The caller can press another key or hang up.
Key 3	**Auto Attendant** The system routes the call to the auto attendant so the caller can enter an extension.	—
Key 4	**Auto Attendant** The system routes the call to the auto attendant so the caller can enter an extension.	—
Key 5	**Play prompt—** Use Text to Speech to say: — *Please leave your name and number in your message.* Then **Go to mailbox number**. Enter the mailbox number or extension for general messages. The system directs the call to this mailbox.	—
Key 6	**Transfer to extension**	—

	Change action or select the prompt dialog	
Menu action	**First perform this action:**	**Then perform this action:**
	Enter the extension of the customer service. The system transfers the call to this extension.	
Key 7	**Subscriber login** Transfer the call to the voice messaging pilot number so that the user can log in to the mailbox. The Instructions do not list this option as this option is only for employees.	—
Key 8	**Hangup** End the call.	—
Key 9	**Not active**	—
Key 0	**Not active**	—

Schedules

Business schedules

The business schedule defines the operating hours for your organization.

If the caller application receives a call within business hours, the caller application plays the Business Hours menu for the caller. Else, the caller application plays the Off Hours menu.

The default business hours are 8:00 a.m. through 5:00 p.m., Monday through Friday. However, you can change these hours in Caller Applications Editor.

Holiday schedules

You can create a menu that the caller application activates only on the dates specified by a holiday schedule. Each holiday schedule is a separate system object that you define once. Any caller application can use the holiday schedule.

A typical deployment has two or three defined holiday schedules. However, there is no restriction on the number of unique holiday schedules that you can create.

Guidelines for holiday schedules

- When you do not need a holiday schedule, use the **None** schedule. You cannot rename the **None** schedule.
- When you create a new holiday schedule, give the holiday schedule a unique descriptive name. For example, *2010 Corporate Calendar*.
- The holiday menu plays for the entire day specified by the holiday schedule. The day starts at 12:00 a.m. and ends at 12:00 a.m. the following day.
- A holiday schedule can include more than one date.
- When you change a holiday schedule, the system automatically updates the caller applications that use the holiday schedule.

Planning a caller application

Caller applications checklist

You must plan the basic properties for the caller application container and menu logic before you create the container in Caller Applications Editor. Use the following checklist as a guide for the tasks that you must complete in Caller Applications Editor..

You must perform the first two tasks in sequence. You can perform the other tasks in any order.

No.	Task	References	✔
1	Create a plan for the caller menus and prompts.	• Worksheet for container properties on page 189 • Worksheet for menus on page 189	
2	Define a location on the storage server for storing mailboxes associated with caller applications.	Creating containers on page 195	
3	Define a caller application container.	Creating containers on page 195	

No.	Task	References	✔
4	Define the schedule for each caller menu.	• Creating business schedules on page 198 • Creating holiday schedules on page 198	
5	Create the call menus.	Creating menus on page 197	
6	Load audio prompts.	Assigning audio prompts to menus on page 199	

Worksheet for container properties

Tip:

You must first create a test mailbox and extension. After your tests are complete, change the **Mailbox number** and **Extension** fields to the production numbers.

Container property	Notes
Name of the caller application	—
Mailbox number	Test: Production:
Extension	Test: Production:
(Optional) Additional extensions associated with the caller application	—
Will the caller application be available in Auto Attendant? If yes, define the pronounceable name.	—
Define the business hours. For example, Monday to Friday, 8:00 a.m. to 5:00 p.m.	—

Worksheet for menus

Use this worksheet to plan the logic for a Business Hours or Off Hours menu. See Example menu on page 185 for an example of a Business Hours menu.

		Complete only for Play Prompt actions	
Prompt or key press	**Menu action (select one)**	**Filename or TTS text**	**Define next action**
On Answer	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Instructions	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 1	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		

		Complete only for Play Prompt actions	
Prompt or key press	**Menu action (select one)**	**Filename or TTS text**	**Define next action**
Key 2	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 3	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 4	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		

		Complete only for Play Prompt actions	
Prompt or key press	**Menu action (select one)**	**Filename or TTS text**	**Define next action**
Key 5	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 6	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 7	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		

		Complete only for Play Prompt actions	
Prompt or key press	**Menu action (select one)**	**Filename or TTS text**	**Define next action**
Key 8	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 9	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 0	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		

Installing Caller Applications Editor

Procedure

1. Open your browser, and type the following URL: `http://<Messaging server>/download/CallerApplicationsEditor.msi`.

   <Messaging server> is the IP address or DNS name of the Messaging server.

2. When the system displays the **File Download** dialog box, click **Run** and then follow the instructions in the Avaya Aura® Messaging Caller Applications Editor Setup wizard.

Changing the Caller Applications password

Use the System Policies Web page to change the Caller Applications administration password. The default password to log in to Caller Applications Editor is `caadmin01`.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Policies**.
2. In the **Caller Applications Administrator** area, enter the new password in the **Password** field.
3. Re-enter the password in the **Confirm password** field.

   For more information, see System Policies field descriptions on page 143.

4. Click **Save**.
   The system saves the settings.

Working in Caller Applications Editor

Logging in to Caller Applications Editor

Before you begin

- All prerequisite software is loaded on to your computer. See System requirements on page 181.
- You know the IP address or DNS name of the storage server.
- You know the password for Caller Application Editor. When you access the software for the first time, the password is `caadmin01`.

Procedure

1. Click **Start** > **All Programs** > **Avaya Connector** > **Avaya AxC CallerApps**.
2. Enter the following information in the Connect to Messaging AxC fields:
   - **AxC address**: The IP address or DNS name of the storage server.
   - **Password**: The password for Caller Applications Editor.
3. Click **OK**.
   Caller Applications Editor displays the IP address for the AxC connector in the title bar and the navigation pane.

Creating containers

When you create the first caller application for your system, Caller Applications Editor prompts you to select a location on the storage server for storing mailboxes associated with caller applications. The location must be different from the location where you store your voice messaging user accounts.

Before you begin

Before you create the first caller application, determine where you want to store the caller application mailboxes.

Procedure

1. In Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. Right-click **Caller Applications**.

3. Select **New** > **Caller Application**.
4. If you are creating the first caller application for the system, identify the location for storing caller application mailboxes.

   Caller Applications Editor only prompts you for a storage location for the first caller application that you create.
5. Enter the appropriate information in the New Caller Application dialog box.

   For more information, see New Caller Application field descriptions on page 196.
6. Click **OK**.
   The system creates the caller application.

Next steps

See Creating menus on page 197.

New Caller Application field descriptions

These fields define the caller application container.

Name	Description
Name	The name of the caller application.
Mailbox number	The mailbox number for the user account associated with the caller application. All mailbox numbers for user accounts must be unique. However, the mailbox number does not have to match the extension.
Include in Auto Attendant Directory	Whether you want to make the caller application accessible through the Auto Attendant directory. If yes, complete the **Pronounceable name** field if you can pronounce the name in different ways.
Extension	The extension that callers dial to reach the caller application. The extension must be unique.
Additional extensions	Any additional extensions that you want to associate with the caller application. Examples of when to enter additional extensions: • When multiple DID numbers access the caller application. • When a caller application migrates from a legacy phone system and the internal

Comments? infodev@avaya.com

Name	Description
	directory supports both the old and the new extensions.
Site	The location of the telephony server to which the caller application belongs. In a multisite configuration, the drop-down list displays all sites in the system.
Pronounceable name	If a user or info mailbox has a name that you can pronounce in different ways, spell the name, as you would pronounce the name. For example, spell Dan DuBois as `Dan Doobwah`. This entry might reduce the number of attempts the Speech Recognition feature makes to match a spoken name to the name in the Auto Attendant directory. You can also enter an alternative name. For example, if the original name for the caller application is *Customer Support*, you can enter *Technical Support* in the field. The speech engine recognizes both the names.

Creating menus

Before you begin

Create a container for the caller application. See Creating containers on page 195.

Procedure

1. In Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. In the Name pane, right-click the caller application and then select **Properties**.
3. Select the **Properties** tab for the menu that you want to create.
4. Use your worksheet to complete the fields.
   Repeat Step 3 and Step 4 for each additional menu.
5. If you are using audio prompts, see Assigning audio prompts to menus on page 199.
6. Click **OK**.
   The system creates the menu.

Creating business schedules

Procedure

1. In Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. In the Name pane, right-click the caller application and then select **Properties**.
3. Select the **Hours** tab.
4. Edit the hours grid.

   Use the drag and drop function of the cursor to select or deselect blocks of time on the hours grid.
5. Click **Apply**.

Creating holiday schedules

About this task

Caller applications only use holiday schedules for the year that you created these holiday schedules. For example, if you create a holiday schedule for Christmas 2011, you must create a new schedule for Christmas 2012.

Procedure

1. In Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. Right-click **Holiday Schedules**.
3. Click **New** > **Holiday schedule**.
   MMC adds a New Holiday Schedule container.
4. Right-click on the **New Holiday Schedule** container.
5. Click **New** > **Holiday**.
6. In the New Holiday Properties dialog box:
   a. Enter a name for the holiday.
   b. Select a date.
   c. Click **OK**.
7. In the Name pane, right-click the newly created holiday object and select **Properties**.
8. Edit the date and description.
9. Click **Apply**.

Repeat steps 4 through step 9 for each additional new holiday that you want to add to the schedule.

Assigning audio prompts to menus

Before you begin

You have access to prerecorded audio prompts in .wav format.

Procedure

1. In Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. In the Name pane, right-click the caller application and then select **Properties**.
3. Select the **Prompts** tab and then click **Add**.
4. Navigate to the folder that contains the prerecorded audio prompts.
5. Select a .wav file.

   You can select multiple files at the same time.
6. Click **OK** to add the files to the caller application.
   The caller application that you selected uses the prompts for any Play Prompt action. See Menu actions on page 184.

   Repeat these steps for each additional caller application.

Deploying a caller application

Before you begin

- Create and test the caller application.
- Reload the User List on each of the application servers each time after you update Caller Application. For more information, see Loading lists on page 175.

Procedure

1. In Caller Applications Editor, open the Properties dialog box for the caller application.
2. Select the **General** tab.
3. Change the **Mailbox number** and **Extension fields** from the test numbers to the production numbers.
4. On each relevant Properties tab, click **Apply**.

The system deploys the caller application to each application server in the cluster.

Chapter 12: Teletypewriter

Teletypewriter overview

TTY is a data terminal that users who are hearing impaired or speech impaired can use to transmit and receive text through a telephone system. You can also refer to a TTY as Telecommunications Device for the Deaf, or TDD. A typical TTY resembles the keyboard of a laptop computer with a one-line or a two-line alphanumeric display. When you do not use the TTY to transmit text, the TTY is silent. As a user types on the device, the TTY emits audio tones that the telephone network transmits.

Not all TTY users transmit and receive messages with TTY devices. Approximately half of the users who rely on TTY devices are hearing impaired, but can speak clearly. These users often prefer to receive messages on their TTY devices and then speak in response. You can refer to this process as Voice Carry Over, or VCO.

Messaging offers the Audix TUI, which provides support for TTY users. The Audix TUI supports many of the features and menus of traditional Audix and Intuity Audix systems.

Messaging supports TTY on the TUI caller interface. The TUI caller interface is the part of the code that allows the user to log into the system. After the user logs in, the system presents the Audix TUI menu. The caller interface is currently Aria-like and the administrator cannot change this behavior.

Messaging does not provide automatic TTY support in Messaging mailboxes. You must enable TTY support in the same way that you configure a mailbox to use a spoken announcement set. For the TTY announcement set, you can also specify the conditions under which the specific mailbox uses TTY-format prompts and menus. Regardless of the selected announcement language, users can record TTY or voice messages.

In Messaging, you can configure mailboxes so that callers can select TTY-format, or voice prompting from the same mailbox. Thus, mailbox owners who receive both TTY and voice calls no longer need different telephone numbers and mailboxes for each type of call.

You must be aware of the following issues that can compromise the use of TTY devices on a Messaging system:

- You must configure the Messaging system to use the G.711 encoding format. The GSM encoding format works well with voice but distorts the TTY tones. For more information, see Ensure voice quality on page 203.
- Under certain conditions, the Messaging system does not support TTY with Internet Protocol (IP) integration. For example, the system does not support IP integration when TTY tones transmit across a wide area network (WAN).

Important information

This topic includes the following information that you need for administering TTY-enabled Messaging systems:

- Setting up a teletypewriter for your system and the user on page 202
- Inform teletypewriter users about the login option on page 203
- Ensure that teletypewriter users receive broadcast messages on page 203
- Ensure voice quality on page 203

Setting up a teletypewriter for your system and the user

Important:

You can associate the site that you create for TTY users with an existing application server that includes another site.

Before you begin

Avaya recommends that you disable speech recognition for TTY users. For more information, see Speech recognition on page 137.

Procedure

1. On the Languages Web page, install the *English (United States) - TTY* language pack. For more information, see Configuring languages on page 68.
2. On the Sites Web page, create a new site for TTY users with the following settings:
   - In the **Main Properties** area, in the **Site Default Language** field, select **English (United States) – TTY**.
   - In the **Auto Attendant** area, in the **Default Language** field, select **English (United States) – TTY**.

Note:

Do not configure:

- TTY as a second language
- Additional languages for TTY users

In Messaging, pilot numbers must be unique for different sites. Hence, for the new site you must create a unique pilot number for voice mail and Auto Attendant.

3. On the Miscellaneous Web page, set the audio encoding format to *G.711*. For more information, see Configuring the miscellaneous information on page 357.
4. In User Preferences, instruct the users to select the language as **English (United States) - TTY**.
   The system defines the default language for user login sessions.

Inform teletypewriter users about the login option

Inform TTY users to log in to the mailbox. For more information, see the *Mailbox access using a phone* section in *Using Avaya Aura® Messaging*.

Ensure that teletypewriter users receive broadcast messages

The Messaging system sends spoken broadcast messages to all mailboxes on the system, including the TTY mailboxes. Ensure that TTY users receive the voice messages in a timely manner.

Ensure voice quality

Messaging systems encode speech and TTY tones digitally for recording, transmission, and storage. Different encoding techniques are available depending on whether you want to maximize audio quality or storage efficiency. The G.711 format provides the highest audio quality especially when voice networks use multiple encodings and decodings. Avaya requires that you use the G.711 encoding format in Messaging systems that support TTY devices.

The G.711 encoding format uses a higher encoding rate than GSM. The G.711 encoding format therefore produces larger files and requires more storage space for messages. Messaging provides customers with adequate storage space for message playback and networking.

Chapter 13: Managing software

Viewing the currently installed software

Use this procedure to view the list of software packages on the Messaging server. You must view this list:

- Before you download additional software packages so you know which packages to download.
- After you install new software packages so you know that the system installed the packages properly.

Procedure

On the **Administration** menu, click **Messaging** > **Software Management** > **List Messaging Software**.

The page displays the installed packages in alphabetical order or installation time. You can change the view by selecting:

- **Display software in alphabetical order**
- **Display software installation time**

Patch installation overview

A Service Pack provides product updates and bug fixes. When a Service Pack is available on the Avaya Support website, the supporting information clearly states the issues addressed in the Service Pack. You must implement the Service Packs even if you are not experiencing any problems. The Service Packs keeps the systems up-to-date and minimizes the likelihood of any future impact from known issues.

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

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

- Messaging
- Communication Manager

You must install the following patches when available:

- Security
- Kernel

To download the latest patches, and to obtain the necessary information, see Avaya Aura® Messaging Release Notes on the Avaya Support website at http://www.avaya.com/support. For more information on installing patches using cdom, see the Messaging implementing or upgrading guide.

Important:

Perform a system backup before applying any patch. When you install the latest patch, the installation program automatically uninstalls the previous patch. If you remove a patch, the removal does not reinstall the previous patch or change the system to the previous state, that is, the state before you installed the patch. To change the system to the previous state, you must reinstall the previous patch.

Caution:

Patch installation process impacts Messaging service availability.

Installing software

The software installation page displays the packages available for installation.

Before you begin

You must perform the following steps using a privileged administrator account with the necessary rights.

- To create a privileged administrator login, see Adding a privileged administrator login on page 30.
- To provide the necessary rights, log in to the SMI as a privileged administrator. Use the Web Access Mask SMI page to create a new mask that has the *Software Install* rights. For more information, see Adding a Web Access Mask on page 329.
- After you create the mask, use the Administrator Accounts SMI page to create a new user or change the properties of an existing user and add the mask that you created to the **Additional groups (profile)** field.

Procedure

1. Perform a full system backup. See Backing up system files on page 213.
2. On the **Administration** menu, click **Messaging** > **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The system lists all the available software packages that you can install, including all software packages and patches that you have previously downloaded.
4. Select the software packages that you want to install.
5. Click **Install selected packages**.

Verifying system installation

About this task

Use the Verify System Installation Web page to confirm that:

- The system installed the primary software packages properly.
- A complete version of each application-specific package exists on the system.

The system performs a series of background checks on the system software. The system checks the content of each installed executable or help file, but not data files, to verify that the files were unchanged.

Procedure

On the **Administration** menu, click **Messaging** > **Software Management** > **Software Verification**.
The Verify System Installation Web page displays each of the primary software packages and protocols installed on the system. The Web page also displays notes on any exceptions.

Installing advanced software

Note:

Do not install advanced software unless Avaya services specifically instruct you to do so.

Use the following instructions to install the required advanced software. Plan to install the software during low usage hours, as most software installations require that the cornerstone is not running.

You can also install additional software packages from a CD inserted into your laptop or from technical support websites.

Before you begin

You must perform the following steps using a privileged administrator account with the necessary rights.

- To create a privileged administrator login, see Adding a privileged administrator login on page 30.
- To provide the necessary rights, log in to the SMI as a privileged administrator. Use the Web Access Mask SMI page to create a new mask that has the *Advanced Software Install* rights. For more information, see Adding a Web Access Mask on page 329.
- After you create the mask , use the Administrator Accounts SMI page to create a new user or change the properties of an existing user and add the mask that you created to the **Additional groups (profile)** field.

Procedure

1. On the **Administration** menu, click **Messaging** > **Software Management** > **Advanced Software Install**.
2. Click **Continue without current system backup**.

   The system lists all the available software packages that you can install, including all software packages and patches that you have previously downloaded.
3. Select the software packages that you want to install.
4. Click **Install selected packages**.

Deleting software packages

Before you begin

You must perform the following steps using a privileged administrator account with the necessary rights.

- To create a privileged administrator login, see Adding a privileged administrator login on page 30.
- To provide the necessary rights, log in to the SMI as a privileged administrator. Use the Web Access Mask SMI page to create a new mask that has the *Software Removal* rights. For more information, see Adding a Web Access Mask on page 329.
- After you create the mask, use the Administrator Accounts SMI page to create a new user or change the properties of an existing user and add the mask that you created to the **Additional groups (profile)** field.

Procedure

1. On the **Administration** menu, click **Messaging** > **Software Management** > **Software Removal**.
2. Select the software packages that you want to delete.
3. Click **Submit**.
   The system deletes the software.

Chapter 14: Back up and restore

Back up and restore overview

Purpose of Backup and Restore

The Messaging server backs up Messaging data over the customer LAN to an external ftp server. The data can be backed up at the same time as the server data, or independently. In the event of a system failure, the system uses the information stored on the external server to restore the system to an operational state. Messaging supports up to 20,000 mailboxes. Messaging data backup might easily reach 50 Gigabytes or more. Customers might be unable to support transfers of single files of this size. Hence, in Messaging, the system automatically divides large data backups into 500 MB files before transfer. Each file transfer might complete in about 5 minutes. Consequently, the network must support a minimum average transfer rate of 1.6 MB/sec. Messaging supports the following backup methods:

- FTP
- SFTP
- SCP

The system administrator who is administering network backups using FTP, SCP, or SFTP must be aware of the possible file storage sizes and the limitations of the storage size on the customer data network.

A system administrator can mitigate the backup file size by:

- Limiting the mailbox size of the user storage, so that users do not have more than 10 minutes of voice storage in their mailbox.
- Limiting the number of days a message can remain in a mailbox before the system deletes the message. Currently, the system default is 45 days, that is, a message remains in the mailbox for 45 days before the system deletes the message. The system automatically deletes messages during the nightly audits after the message age equals the administered number of days.

Data that you can back up and restore

You can back up any combination of the following Messaging data types at any time manually, Backup Now, or according to a schedule automatically, Scheduled Backup. The data types are:

- Translations
- Announcements

- Messaging names
- Messaging greetings and messages

Note:

The system does not include language packs in the backup. Hence, you must install language packs on each application server.

Translations

Translations comprise of the following data:

- Detailed system data on shared memory, speech file system pointers
- Alarm management information
- A list of enabled features
- A list of installed software
- Messaging digital networking connectivity and communication information
- Message headers, mailing lists, user profiles including automated attendant administration, and message-waiting indicator status
- Telephony server integration parameters
- Hard disk configuration

Besides scheduled backups, you can also perform backups whenever you make extensive changes to user profiles.

Announcements

Announcements are prompts and phrases that guide a user through the Messaging application. This data type does not require a backup unless the system has customized announcements that changed recently. If you do not use customized announcements, a backup of announcements exists on the Avaya support site. See https://support.avaya.com.

Messaging names

The Messaging names data type contains recorded user names. You must perform a backup of this data type after you record additional user names.

Voice messages

Voice messages are recorded messages that users have received and retained. This includes the primary voice greeting, multiple personal greetings, and automated attendant menus and messages.

FTP server availability

If the FTP server is unavailable at the time of the backup, the backup fails. You must ensure that the maintenance on the FTP server does not coincide with backup timings. A backup requires 30 minutes or more, depending on the size of your files and the network traffic.

About restoring backed-up system files

The system uses the Messaging information stored on a server during data backups to restore the system to an operational state. Use the **View/Restore Data** Web page to restore backed-up system files.

Restore backups when an alarm repair action directs you to do so.

Backup verification

You must verify the success of each backup you run. A backup can include a variety of data types, in addition to Messaging server data. The View Backup Log screen, available from the Server (Maintenance) Web page, displays all backed up files. You can open any file and view the data types that the file contains.

Note:

Backups cannot be partially successful. A Messaging backup is successful only if the backup includes all the data that you selected to back up.

If you perform the operations of backup and restore on the storage server, the Sites Web page data or provisioning data that the storage server uses is not the same as used by the application servers. The difference in data results in unexpected behavior in the operations on the application server.

Hence, if you perform the operations of backup and restore on the storage server, you must restart the Messaging server. By restarting the Messaging server, the system forces the application server to refresh the Sites Web page data in the cache that the application server maintains.

Backing up system files

You can manually backup your system at any time or you can schedule routine backups. A manual backup is also called an attended backup. Use the following instructions to perform attended backups.

Procedure

1. Stop Messaging. For more information, see Stopping on page 377.
2. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **Backup Now**.
   The system displays the **Backup Now** Web page.
3. In the **Data Sets** area, select **Specify Data Sets**. Then select:
   - **Server and System Files**
   - **Security File**
   - **Messaging**

4. In the **Messaging** area, select **Messaging Application, Translations, Names, and Messages**.
5. In the **Backup Method** area, select **Network Device** and then complete the following fields:
   a. **Method**
   b. **User Name**
   c. **Password**
   d. **Host Name**
   e. **Directory**
6. In the **Encryption** area, select **Encrypt backup using pass phrase** and then enter a phrase.
7. Click **Start Backup**.
   For more information, see Backup Now field descriptions on page 214.

Backup Now field descriptions

Settings	Description
Specify Data Sets	The data sets that you want to back up. The available options are: • **Server and System Files**: Back up the variable information to configure the server for a particular installation. • **Security File**: Back up the variable information to maintain security of the server. • **Messaging**: Back up one of the following Messaging options: - **Messaging Application, Translations and Messages** - **Messaging Application, Translations, Names, and Messages** - **Messaging Application, Translations and Names** - **Messaging Application and Translations** - **Messaging Application**

Settings	Description
Full Backup	A full backup includes security data sets and files that configure both the Linux operating system and the applications. A **Full Backup** does not include any of the Messaging data sets.
Backup Method	
Method	The following methods are available for backup: • **SCP**: A means of securely transferring computer files between a local and a remote host, or between two remote hosts, using the Secure Shell (SSH) protocol. • **FTP**: When you choose this option, you must also enter a user name, password, host name, and directory. The default directory for backup data on the FTP server is `/var/home/ftp`. If you want to use the default directory, enter a forward slash (/) in the directory field. You must start the FTP server before backing up data. • **SFTP**: A network protocol that provides file transfers over data streams. The system adds the SFTP client to all Linux platforms.
User Name	The user name for storing the backup.
Password	The password for storing the backup.
Host Name	The host name.
Directory	The backup is stored on this network directory.
Encryption	
Encrypt backup using pass phrase	Defines if you want to encrypt the backup data. The pass phrase can be an arbitrary string of 15 to 256 characters. The pass phrase can contain any characters except the following: single quote ('), ampersand (&), back slash (\), single back quote (`), quote ("), and percent sign (%).

Backing up System Platform

About this task

Use this procedure to back up configuration information for System Platform and the Messaging template. Use the System Platform Web Console to back up the files.

Important:

The backup file size can reach 3 GB. Ensure that you have that enough free space at the location where you are storing the backup archive.

Procedure

1. Log on to the System Platform Web Console.
2. Click **Server Management** > **Backup/Restore**.
3. Click **Backup**.
4. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
5. Select the location to store or send the backup files:
   - **Local**: Stores the backup archive file on System Platform in the `/vspdata/backup/archive` directory.
   - **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server.
   - **Email**: Sends the backup archive file to the e-mail address that you specify as well as stores the file on the System Platform server.

     Note:

     Avaya does not recommend that you use the **Email** option due to the large size of backup files. The backup file size can reach 3 GB.
6. Enter other information as appropriate.
7. Click **Backup Now**.

Backup field descriptions

Field Name	Description
Backup Method	Select a location to send the backup file: • **Local**: Stores the backup archive file on System Platform in the **/vspdata/backup/archive** directory. • **SFTP**: Stores the backup archive file on the designated SFTP host server as well as on the System Platform server. Enter the hostname, directory, user name, and password for the SFTP server. • **Email**: Sends the backup archive file to the email address that you specify, as well as stores the file on the System Platform server. Enter the email address and the server address of the recipient.
Backup Now	Starts the backup operation.

Scheduled backups

Use Backup Now when you want to back up system data immediately. For example, you might want to back up data soon after you install the Messaging server or the Messaging system. Additionally, you might want to run the backup procedure just before making a change to your system. Running the backup ensures that the most recent data is backed up, including data that is new since the last scheduled backup was run.

Additionally, the Messaging backup files can be quite large. As a result, your LAN network connection can fail during the backup. In this case, you must run a scheduled backup, which allows the Messaging server to handle breaks in the LAN connection, and create a successful backup. To run a scheduled backup in case of a failed backup, set the schedule to run on the current day and 5 or 10 minutes in the future. See Adding a new backup schedule on page 218.

Adding a new backup schedule

About this task

To create a backup schedule, you must first decide what type of data you want to back up. You must then indicate the days and time you want the schedule to run and the destination to which you want the backup files sent.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **Schedule Backup**.

   The system displays the Schedule Backup Web page.

   If backups are already scheduled, the screen lists the current backup schedules. Look at the schedules carefully to determine what backup schedule you want to add.

   If this is the first backup schedule that you are creating, the Schedule Backup Web page displays a message stating that there is no record of any backup schedule.

2. Click **Add**.

   The system displays the Add New Schedule Web page.

3. Select **Specify Data Sets**.
4. Select **Messaging**.
5. Select **Messaging Application, Translations, Names, and Messages**.
6. Select a backup method.

   a. Enter **User Name**.
   b. Enter **Password**.
   c. Enter **Host Name**.
   d. Enter **Directory**.

7. If you want to encrypt the backup data, select the check box in the **Encryption** area of the screen and enter a pass phrase using an arbitrary string of 15 to 256 characters.

   A pass phrase is similar to a password in usage, but is generally longer for added security.

   You must encrypt the backup data. You must remember the pass phrase because you cannot restore the data without the pass phrase.

8. 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 **Start Time** field.

   You can select multiple days but only one time for the backup schedule to run.

9. Click **Add New Schedule** to save the schedule you just created.

The system displays the Schedule Backup Web page with the new backup schedule added to the schedule list.

Changing a backup schedule

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **Schedule Backup**.

   The system displays the Schedule Backup Web page.

   If backups are already scheduled, the screen lists the current backup schedules. Look at the schedules carefully to determine which backup schedule you want to change.

   If there is no backup schedule, the Schedule Backup Web page displays a message stating that there is no record of any backup schedule.

2. From the list containing the current scheduled backups, select the backup schedule you want to change and click **Change**.

   The system displays the Change Current Schedule Web page.

3. Change the information, as appropriate.
4. Click **Change Schedule**.

Deleting a backup schedule

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **Schedule Backup**.

   The system displays the Schedule Backup Web page.

   If backups are already scheduled, the screen lists the current backup schedules. Look at the schedules carefully to determine which backup schedule you want to delete.

   If there are no backup schedules, the Schedule Backup Web page displays a message stating that there is no record of any backup schedule.

2. From the list containing the current scheduled backups, select the backup schedule you want to delete.
3. Click **Remove**.

The system updates the scheduled backup list.

Viewing backup history

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **Backup History**.

   The system displays the Backup History Web page with a list of the 15 most recent backups.

2. To check the status of a specific backup, select the backup and click **Check Status**.
   The system displays the Backup History Results Web page with the details of the selected backup.

Viewing backup logs

When you back up data, the system creates an image as a tar file that contains information, such as the type of data sets that the system backed up, whether the backup was successful, and and how the system recorded the data. Use the Backup Logs Web page to verify the success or failure of a backup.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **Backup Logs**.
2. On the Backup Logs Web page, check the backup log that you want to preview or restore. To select the log, click the option.

   If no entries exist in the backup log, you will see a message stating that there is no record of any backup.

3. Click **View**.

   The system displays the View/Restore Data Results Web page.

4. Enter the **Username** and **Password** for file transfer settings.
5. Click **Preview**.

Backup Logs field descriptions

Name	Description
Data Set	The data set for which you performed the backup.
File Size	The file size of the backup.
Date	The date on which you performed the backup.
Time	The time at which you performed the backup.
Status	The status of the backup.
Destination	The destination where you saved the backup.

Performing a restore

About this task

Note:

You must stop your Messaging system before you restore the data. For more information, see Stopping Messaging on page 377.

The time required for a restore depends on the amount of data on the system and the speed of the LAN traffic. Perform the following procedure for both attended and unattended backups.

Procedure

1. Stop the Messaging software. For more information, see Stopping Messaging on page 377.
2. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **View/Restore Data**.

   The system displays the View/Restore Data Web page.
3. In the **View current backup contents in** area, select **Network Device** or **Local Directory**. Use the same information that you used when you backed up the data to complete the following fields in case you selected **Network Device**:

a. **Method**
b. **User Name**
c. **Password**
d. **Host Name**
e. **Directory**

4. Click **View**.

   The View/Restore Data Results Web page lists the backup images stored in the location that you specified. The system lists the most recent backups at the bottom of the list.

   You must select a backup image before you click **View**, or the system displays an error message. To clear the error message, click **Back** on the browser and then select a backup image.

5. To select the backup image you want to view or restore, click the corresponding option.

   If you want to restore both the Messaging server data sets as well as the Messaging data sets, you must restore the Messaging 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 **Force restore if backup version mismatch** if the backup version mismatches and **Force Restore if server name mismatch** if the server name mismatches.

6. Click one of the following:

   • Preview. Use **Preview** if you are unsure that 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 has 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

   - Click **Restore** on the 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 **Force restore if backup version mismatch** if there is a mismatch in the backup version, and **Force Restore if server name mismatch** if there is a mismatch in the server name.

- Restore. When you click **Restore**, the system displays the View/Restore Data Results Web page which displays whether the restore procedure was successful.

7. Do one of the following:
   - If you do not have any remote networked machines, continue with Step 8.
   - If you have remote networked machines, do the following:

   a. Log off the Messaging server.
   b. Log in to the Messaging Web page.
   c. Run a manual update to and from all remote networked machines to correct any database inconsistencies.

      For more information, see Running a remote update manually on page 153.
   d. Continue with Step 8.
8. Restart the Messaging software. For more information, see Starting Messaging on page 377.

View/Restore Data field descriptions

Name	Description
Network Device	The network device on which you stored the backup content.
Method	The backup method. The options are: • **sftp** • **ftp** • **scp**
User Name	The user name for accessing the backup.
Password	The password for accessing the backup.
Host Name	The host name.
Directory	The network directory on which you stored the backup content.
Local Directory	The local directory on which you stored the backup content.

Viewing restore history

The Restore History Web page displays the 15 most recent restores, which the system identifies by the server name, date, and time of the backup and the process ID.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **Restore History**.

   The Restore History Web page displays a list of the 15 most recent restores.
2. To check the status of a specific restore, select the restore and click **Check Status**.

Storage space calculation

The following formula estimates how much space the system requires for the LAN backup for a night based on the number of users, the average number of messages and greetings measured in minutes, and the audio encoding format.

Space used each night = `100MB + 0.05MB*(L+R) + (0.1MB*M*L*F)` where:

- MB represents a unit of megabytes.
- L is the number of local users existing on the system that night.
- R is the number of remote users existing on the system that night.
- M is the average number of minutes of messages per mailbox.
- F equals 1 if the system uses GSM encoding, and F equals 5 if the system uses G.711 encoding.

Example

A G.711 system with 2,000 local users with 5 minutes of messages/greetings and 50,000 remote users occupies approximately:

= 100MB + 0.05MB*(2000+50000) + (0.1MB*5*2000*5)

= 100 MB + 2600 MB + 5000 MB

= 7.7 GB.

Comments? infodev@avaya.com

Restoring System Platform configuration information

About this task

Note:

You cannot restore an older version of System Platform from a backup set created on a newer version of System Platform.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
   The Restore page displays a list of previously backed up archives on the System Platform system.
3. Select an archive file from the list, and then click **Restore** to restore from the selected archive.

   The restore progress window opens in the **Restore** tab, displaying restore event messages with corresponding timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - A system error condition abruptly halts the operation. In this case, contact Avaya Support at http://support.avaya.com.

   When the restore progress window displays a message indicating successful completion of the operation, the system restarts and you must log on again to the System Platform Web Console.

System Platform restore field descriptions

Field Names	Descriptions
Restore from	Select the location of the backup archive file from which you must restore configuration information. • **Local**: Restores from a file on System Platform. If you select this option, the Restore page displays a list of previously

Field Names	Descriptions
	backed up archives on the System Platform system. • **SFTP**: Restores from a file on a remote server. If you select this option, enter the hostname or IP address of the remote server, directory where the archive file is located, and user name and password for the SFTP server. • **Upload**: Restores from a file on your computer.
Archive Filename	Filenames of the backup archive files at the location you specify.
Archive Date	Date that the file was created.
Selection	Select this check box to restore from the archive file.
Restore History	Displays the restore history for the last ten restores. If an error occurred during the last restore, the system directs you to this page after login and continues to display an error message until a restore is successful.

Viewing System Platform restore history

About this task

Use this procedure to view the last 10 restores executed and their status. If the last restore failed, the system automatically redirects you to the Restore page after login and displays the following message: `Last Restore Failed`. The system continues to display the message until a restore is successful

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
3. On the Restore page, select the **Restore History** option.

Comments? infodev@avaya.com

Chapter 15: Alarms

Alarms overview

The Maintenance log records system errors. The Messaging system tries to diagnose and isolate these errors from the system and sends an alarm to the Alarm log if the Messaging system is unable to correct the error automatically.

The system displays all alarms on the **Messaging** > **Logs** > **Alarm** Web page. The content in the alarm log represents all significant problems that the system detects. Therefore, the alarm log is a good starting point for troubleshooting the system.

The Messaging alarm logs are of the following types:

- Active alarm: The alarm indicates a current problem in the system.
- Resolved alarm: The system has corrected the alarm automatically or through a repair procedure.

Alarm severity is of the following levels:

- Major Alarms: These alarms indicate problems that could affect key system components or features. For example, if more than 25% of the voice ports are out of service, the system generates a major alarm. Major alarms are repairable by technicians.
- Minor Alarms: These alarms indicate problems that could affect full service but are not critical to system operation. For example, if a network connection problem occurs, the system generates a minor alarm. Minor alarms are repairable by technicians.
- Warning alarms: These alarms indicate problems that could potentially affect system service if the alarms are not resolved. For example, if the customer system administrator does not create a trusted server password and a trusted server tries to log in, the system generates a warning alarm. Warning alarms are repairable by customers.

When an active alarm is resolved, the alarm status changes from Active to Resolved.

Alarm Resolution

If the customer purchases a maintenance service contract and activates the alarm origination feature, the system automatically sends major and minor alarms to a remote service center for correction. Warning alarms are not sent to the remote service center.

Alarm Notification

To check alarm notifications, you must check the administrator log and the alarm log daily, either from the Messaging administration screens or from the alarm log on the Messaging

server. Active alarms and new entries in the administrator's log are noted on the STATUS line.

For detailed information on the alarms and events, see *Avaya Aura® Messaging Alarms and Events*.

Important:

The STATUS line displays multiple levels of alarms. The alarm level is important because the alarm level classifies problems within the system so that the most severe problems are worked on first. In most cases, the alarm level also marks the area of responsibility between the system administrator for warning alarms and the remote service center for major and minor alarms.

Alarm notifications

The application server, storage server, and AxC generate system alarms and error logs. You can view these using the SMI screens.

You can send notifications generated by alarms to any of the following recipients:

- Avaya services
- A customer through a Network Management Station (NMS)
- Avaya partners

  Note:

  Avaya partners must gain access to the Messaging system to receive these notifications.

- Avaya Fault and Performance Manager through Secure Services Gateway (SSG) or Avaya Proxy Agent

Messaging uses the following serviceability agents to send alarm notifications to a service organization:

- SAL: The serviceability solution for support and remote management of a variety of devices and products. SAL provides remote access and alarm reception capabilities. SAL uses the existing Internet connectivity of a customer to facilitate remote support from Avaya. All communication is outbound from the environment of the customer over port 443 and uses encapsulated Hypertext Transfer Protocol Secure (HTTPS).
- SAL Gateway: A software package that facilitates remote access to support personnel and tools that must gain access to supported devices. The administrator installs the SAL Gateway on a Linux® operating system in the customer network. The SAL Gateway acts as an agent on behalf of several managed elements. The application server sends the alarms to a SAL Gateway server. The administrator configures the SAL Gateway server

to forward the alarms to various NMS destinations. A SAL Gateway is also included in the CDOM on the server that runs Messaging.

Viewing current alarms

Use the Current Alarms Web page to view a list of alarms and the source of the alarms. The system displays the alarms in chronological order beginning with the most recent alarm.

Before you begin

The telephony application must be running.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Current Alarms**.
2. Check for alarms in **Messaging Alarms**.

Current Alarms field descriptions

Field Name	Description
Product ID	A number that uniquely identifies the server.
Messaging Product ID	A number that uniquely identifies the Messaging product.
Alarm	The alarm summary. If no alarms exist, the system displays the following message: `No MESSAGING Alarms`. If the system displays no alarms, continue with your System Management Interface (SMI) activities.
Server	The outstanding alarms related to the operating system and the support software.
CommunicaMgr	The outstanding alarms related to the call-processing application.
Messaging	The outstanding alarms related to the Messaging system.
Minor	The alarm is a minor alarm.

Field Name	Description
Major	The alarm is a major alarm.
ID	A unique identification number assigned to the alarm.
APP	The name of the application.
Source	The abbreviated name of the software module that is responsible for generating the alarm. The options are: • **All**. All applications • **EL**: Enhanced-List Application • **IM**: Internet Messaging • **LD**: LDAP • **MG**: Messaging • **MT**: Maintenance • **SM**: Station Manager • **VM**: Messaging • **VP**: Voice Platform
EvtID	The number used to identify a particular event from a source that generated the alarm.
Lvl	The level of the alarm. The options are: • **MIN** • **MAJ** • **WARN**
Ack	The status that indicates that Initialization and Administration System (INADS) has acknowledged the alarm. The options are: • **Y**: Yes • **N**: No
Location	The location from where the alarm originated.
Date	A time stamp assigned to the alarm at the time of origination.

Configuring certificate alarms

The Certificate Alarms Web page enables the system administrator to generate early notifications of a certificate that expire in the future. Use this page to configure optional alarms for each of the certificates individually. The system generates a major alarm seven days before and on the day that a certificate on the server expires. You cannot configure or disable this major alarm from the Certificate Alarms Web page and must either delete or replace the expired certificate.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Certificate Alarms** .
2. Select the required check box to configure alarms prior to certificate expiration.
3. Click **Submit**.

Certificate Alarms field descriptions

Name	Description
Enable a _ alarm _ (61–180) days before to certificate expiration.	Configure a warning or minor alarm prior to 61–180 days from the day of certificate expiration.
Enable a _ alarm _ (31–60) days before to certificate expiration.	Configure a warning, major, or minor alarm prior to 31–60 days from the day of certificate expiration.
Enable a _ alarm _ (8–30) days before to certificate expiration.	Configure a major or minor alarm prior to 8–30 days from the day of certificate expiration.

Viewing the alarm summary

Procedure

On the **Administration** menu, click **Messaging** > **Server Information** > **Alarm Summary**.

Alarm Summary field descriptions

Name	Description
System Name	The system name or IP address.
System Time	The system time.
Web Server Status	The status of the Web server.
Message Server Status	The status of the Messaging server.
Number of Major Alarms	The number of alarms that indicate problems that could affect key system components or features.
Number of Minor Alarms	The number of alarms that indicate problems that could affect full service but are not critical to system operation.
Number of Warning Alarms	The number of alarms that indicate problems that could potentially affect system service if not resolved.
Number of entries in the Administrator's Log	The number of entries in the administrators log.

SNMP Traps

Use the SNMP Traps Web page to configure destinations for SNMP traps and notable events on the corporate network. To collect the SNMP messages, there must be a corporate NMS. In addition, you must enable the SNMP ports on the Ethernet interface to the corporate LAN.

Configuring SNMP trap destinations

Before you begin

Before making any configuration changes, ensure that Master Agent is in the **Down** state. The SNMP Traps Web page displays the status of Master Agent. After you complete the configuration, change the status of Master Agent to the **UP** state. You must make all configuration changes in the SNMP Agents and SNMP Traps Web pages before starting Master Agent. Use the Agent Status Web page to start or stop Master Agent. For more information, see Viewing and changing the agent status on page 242.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **SNMP Traps**.
   The system displays the SNMP Traps Web page that displays the existing SNMP traps and the status of Master Agent.
2. Click **Add/Change**.
3. Enter the appropriate information in the fields.
   For more information, see Configure SNMP trap destinations field descriptions on page 233.
4. Click **Submit**.

Configure SNMP trap destinations field descriptions

Field Name	Description
SNMP Version	The three final fields on this page are blank if you use SNMP Version 1 or Version 2c.
Status	If you enable this field, traps or inform requests are sent to a destination. If you disable this field, the system keeps the configuration data in the file and stops sending traps and informs.
IP address	The IP address of the NMS destination or SAL Gateway.
Notification	Displays traps or inform requests.

Field Name	Description
Community Name	The authentication mechanism used by different SNMP versions. **Community Name Authentication** is a plain text string used for SNMP Version 1 and Version 2c.
User Name	User Name is part of the user-based security model for SNMP Version 3. This character string indicates the user who is authorized to send traps to the destination.
Authentication Protocol	The protocol used for authentication. The options are: • none • MD5 • SHA
Authentication Password	The password for the user specified in the **User Name** field. This password is used to digitally sign SNMP Version 3 traps.
Privacy Protocol	The privacy protocol. The options are: • none • DES • 3DES • AES128 • AES192 • AES256
Privacy Password	The password for the user specified in the **User Name** field. This password is used to encrypt SNMP Version 3 traps.
Engine ID	The engine ID.

Changing an administered SNMP trap

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **SNMP Traps**.
2. Check the status of Master Agent.
   Master Agent status must be in **Down** state before you make changes in the SNMP Traps Web page. If **Master Agent status** is **Down**, see step 4.
3. If **Master Agent status** is **UP**, perform the following:
   a. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Agent Status**.
   b. On the Agent Status Web page, click **Stop Master Agent**.
   c. After **Master Agent status** is **Down**, on the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **SNMP Traps**.
4. In the **Current Settings** area on the SNMP Traps Web page, select the check box associated with the trap that you want to change.
5. Click **Add/Change**.
6. Make changes to the trap destination and click **Submit**.
7. After changing the trap destinations, you must restart Master Agent.

Next steps

1. To start Master Agent, on the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Agent Status**.
2. Click **Start Master Agent**.

Deleting an administered SNMP trap

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **SNMP Traps**.
2. Check the status of Master Agent.
   Master Agent status must be in **Down** state before you make changes to the SNMP Traps Web page. If **Master Agent status** is **Down**, see step 4.

3. If **Master Agent status** is **UP**, perform the following:
   a. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Agent Status**.
   b. On the Agent Status Web page, click **Stop Master Agent**.
   c. After **Master Agent status** is **Down**, on the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **SNMP Traps**.
4. In the **Current Settings** area on the SNMP Traps Web page, select the check box associated with the trap that you want to delete.
5. Click **Delete**.
   The SNMP Traps Web page displays the confirmation message for deletion of the destination from the configuration file.
6. Click **Delete**.
7. After deleting the trap destinations, you must restart Master Agent.

Next steps

1. To start Master Agent, on the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Agent Status**.
2. Click **Start Master Agent**.

SNMP filter administration

Use the Filters Web page to perform the following tasks:

- Add an SNMP filter
- Change an SNMP filter
- Delete one or all SNMP filters
- Customer Alarm Reporting Options

The filters are used for Messaging and for determining which alarms are sent as traps to the trap receivers that are administered using the SNMP Traps Web page. For more information on administering SNMP traps, see SNMP Traps on page 232.

Important:

The system does not display the filters created by Avaya Fault and Performance Manager (FPM) on the Filters Web page. If you are using FPM, create the filters using the FPM application. The FPM application provides some additional capabilities that are unavailable using the Filters Web page.

Adding an SNMP filter

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Filters**.
2. Click **Add**.
3. Enter the appropriate information in the fields.
   For more information, see Add Filter field descriptions on page 238.
4. Click **Add**.
   The Filters Web page displays the new filter.

Changing an SNMP filter

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Filters**.
2. Select the check box adjacent to the filter that you want to change and click **Change**.
3. Make the desired changes to the filter and click **Change**.
   The Filters Web page displays the changes made to the filter.

Deleting one or all SNMP filters

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Filters**.
2. To delete all filters, click **Delete All**.
   The system displays a warning message to confirm whether you want to delete all filters. To continue, click **OK**. The system displays the Filters Web page.
3. To delete one filter, select the check box adjacent to the filter that you want to delete and click **Delete**.

The system displays a warning message to confirm whether you want to delete the selected filter. To continue, click **OK**. The system displays the Filters Web page.

Add Filter field descriptions

Name	Description
Severity	Select an alarm severity that is sent as a trap: • **Active** • **Major** • **Minor** • **Warning** • **Resolved**
Category	Select the alarm category for the filter from the drop-down menu.
MO-Type	The options that the system displays are based on the **Category** that you select.
MO Location	Select an **MO Location** from the following list: • **Cabinet** • **Media Gateway** • **Port** • **Board Location** • **Extension** • **Trunk Group/Member** • **None** • **All**

Comments? infodev@avaya.com

Administering an SNMP Agent

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **SNMP Agents**.
2. Check the status of Master Agent.
   Master Agent status must be in **Down** state before you make changes to the SNMP Agents Web page. If **Master Agent status** is **Down**, see step 4.
3. If **Master Agent status** is **UP**, perform the following:
   a. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Agent Status**.
   b. On the Agent Status Web page, click **Stop Master Agent**.
   c. After **Master Agent status** is **Down**, on the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **SNMP Agents**.
4. Enter the appropriate information in the fields.
   For more information on the fields, see SNMP Agents field descriptions on page 240.
5. To save the changes, click **Submit**.
6. After adding the SNMP Agent, you must restart Master Agent.
   a. To start Master Agent, on the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Agent Status**.
   b. Click **Start Master Agent**.

Important:

You can use the Agent Status Web page to change the state of Master Agent and to check the state of the subagents. If the subagent is connected to Master Agent, the status of each subagent is **UP**. If the status of Master Agent is **Down** and the status of the subagent is **UP**, the subagent is not connected to Master Agent.

SNMP Agents field descriptions

Field Name	Description
IP Addresses for SNMP Access	Select one of the following options: • **No Access**: Restrict all IP addresses from talking to the SNMP agent. • **Any IP address**: Allow all IP addresses to access the SNMP agent. • **Following IP addresses**: You can specify up to five IP addresses that have permission to access the SNMP agent.
SNMP Version 1: Community Name (read-only)	Enter a community name and select **enabled** or **disabled** from the drop-down list. **Community Name** is a plain text string used for SNMP Version 1. When you select this option, the community or the user can only query for information (SNMPGETs). If the SNMP Version 1 is enabled, SNMP Version 1 can communicate with the SNMP agents on the server.
SNMP Version 1: Community Name (read-write)	Enter a community name and select **enabled** or **disabled** from the drop-down list. **Community Name** is a plain text string used for SNMP Version 1. When you select this option, the community or the user can query for information and send commands to the agents (SNMPSETs).
SNMP Version 2c: Community Name (read-only)	Enter a community name and select **enabled** or **disabled** from the drop-down list. **Community Name** is a plain text string used for SNMP Version 2c. When you select this option, the community or the user can only query for information (SNMPGETs). If the SNMP Version 2c is enabled, SNMP Version 2c can communicate with the SNMP agents on the server.
SNMP Version 2c: Community Name (read-write)	Enter a community name and select **enabled** or **disabled** from the drop-down list.

Field Name	Description
	Community Name is a plain text string used for SNMP Version 2c. When you select this option, the community or the user can query for information and send commands to the agents (SNMPSETs).
SNMP Version 3	SNMP Version 3 provides the same data retrieval facilities as SNMP Version 1 and SNMP Version 2c with additional security. A user name, authentication protocol, authentication password, privacy protocol, and privacy password are used to provide a secure method of authenticating the information so the device knows whether to respond to the query or not.
User (read-only)	Select **enabled** or **disabled** from the drop-down list. Entering a user name, authentication protocol, authentication password, privacy protocol, and privacy password in this section provides the user with read functionality only.
User (read-write)	Select **enabled** or **disabled** from the drop-down list. Entering a user name, authentication protocol, authentication password, privacy protocol, and privacy password in this section provides the user with read and write functionality.
User Name	User Name is part of the user-based security model for SNMP Version 3. The user name can be a maximum of 50 characters excluding quotation marks.
Authentication Protocol	Select an authentication protocol from the drop-down list.
Authentication Password	Enter a password for authenticating the user. The user name can be a maximum of 50 characters excluding quotation marks.
Privacy Protocol	Select a privacy protocol from the drop-down list.
Privacy Password	Enter a password for privacy. The privacy password can contain 8 to 50 characters excluding quotation marks.

Viewing and changing the agent status

The Agent Status Web page displays the current state of Master Agent and the sub agents. Use this page to start or stop Master Agent.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **Agent Status**.
   The Agent Status Web page displays the current status of Master Agent and Sub Agents.

   If the status of Master Agent is **Up**, the page displays the **Stop Master Agent** button. If the status of Master Agent is **Down**, the page displays the **Start Master Agent** button.
2. To change the status, click **Stop Master Agent** or **Start Master Agent**.

Sending a test trap

Use the SNMP Test Web page to send a test trap to the configured SNMP trap receiver or receivers.

Note:

When you request a test trap, ensure that the configured SNMP Trap receivers receive the test trap.

Caution:

The default firewall setup allows outgoing SNMP traps. However, the test may be invalid if the firewall has been altered in a way that does not allow outgoing SNMP traps.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Alarms** > **SNMP Test**.
2. To send a test trap, click **Generate Test Trap**.

Chapter 16: Logs

Logs overview

There are two types of logs, system and Messaging.

The system logs provide logs for network problems, security issues, system reboots, and so on.

The Messaging system uses a series of logs as the central collection point for information flowing from all Messaging features and feature packages. These logs provide a system wide view of activities, errors, and alarms.

Messages in the logs range in importance from informational to critical. The logs vary based on login type and information type. The current system uses the following types of logs:

- Administration history log: Identifies administrative events that occur on the system. These events include information about any changes to the system, such as logons, command line entries, reports, or changes to software.
- Administrator's log: Records informational messages that may require action by the Messaging system administrator. These messages might simply log a successful nightly backup, or alert the system administrator that the system is low on disk space. The administrator's log is accessible to the vm, sa, and craft logins.
- Alarm log: Indicates a service-affecting or potentially service-affecting problem with the system. The alarm log records major, minor, and warning alarms generated by the system. If you register the system with Avaya Remote Service Center, the system automatically notifies a designated remote service center of all major and minor alarms by using the modem. The customer is responsible for resolving all warning alarms. The alarm log is accessible to the vm, sa, and craft logins.
- Software management logs: Includes information about the installation, update, and deletion of software packages.
- Maintenance log: Records error occurrences, error resolutions, and informational events that can help Professional Services troubleshoot an alarm. The maintenance log is accessible to the vm, sa, and craft logins.
- IMAP/SMTP messaging log: Includes information about the status of each email process.
- Enhanced-List delivery failure log: Provides information on failed ELA deliveries.

- User activity log: Records a list of Messaging mailbox-related events. For example, logins and message creation, receipt, and deletion. This log is useful for responding to problems reported by the user. The activity log is accessible to the vm, sa, and craft logins.
- System log filter: Provides you access to the full system log with advanced filtering options to zoom in on specific constraints.
- Call records: Displays all incoming and outgoing phone activities on the application server.
- Reporting logs: There are two types of reporting logs:
  - Audit log: The audit log is a historical log of cluster configurations in the application server. The audit log tracks all configuration changes made to the system.
  - Port usage logs: The system creates port usage logs and saves the logs daily on the application server in comma-separated value (.csv) format.
- Diagnostics results: These are the results generated by the application server diagnostics. All diagnostics results for a given day are stored in a single log file.
- Call logs: The call logs provide traces of individual calls for application tuning.

Viewing the system logs

The System Logs Web page provides logs for multiple purposes, such as reporting network problems, security issues, and system reboots. You can also request log data for a specific date and time.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Diagnostics** > **System Logs**.
2. Select one of the following:
   - In the **Select Log Types** area, select a log type or types.
   - In the **Select a View** area, select a view.
3. Select an event range.
4. To further limit your search, you can select the **Match Pattern** check box and enter a keyword in the field.
   For example, a name or message type.
5. In the **Display Format** area, select the display options.
   - In the **Number of Lines** field, enter the number of lines you want to view at one time.
   - To view the most recent text line, select **Newest First**.

- To view the text without the header, select **Remove Header**.

6. Click **View Log**.
   The system displays the logs.

System Logs field descriptions

Field	Description
Select Log Types (multiple log output will be merged)	
Logmanager debug trace	Provides information about Messaging and High Availability Platform software, such as restarts, initializations, and shutdowns, process errors, system alarms, and communication with external gateways and port networks. The log rolls over when the log reaches its size limit.
Linux syslog	Linux and platform software use this log. The log includes Messaging boot information, kernel messages, platform alarms, Messaging alarms, Messaging IP events (if enabled), cron jobs, and general Linux information messages.
Linux access security log	The log includes information pertaining to logon connections to the Linux system. Actions logged in this file include opening or closing an SSH session and modem messages.
Linux login/ logout/reboot log	The log includes information about Linux logon and logout procedures, as well as system reboots.
Linux file transfer log	The log includes information about files copied to or retrieved from the system. The log indicates the time, user, and files that were copied to or retrieved from the system.
Watchdog logs	Only the watchdog process updates this log. The log contains information about application starts, restarts, failures, shutdowns, heart beating, and Linux reboots. The log also contains information about processes that use excessive CPU cycles. The watchdog logs do not contain specific information about Messaging. If you need information about processes relating to call processing, see the logmanager debug trace log.
Platform command history log	The log includes information about Web page access, Web page activity, and bash commands. Use the *bashhis* view to display just the bash commands.
HTTP/web server error log	These are errors and events generated by the Web platform server and include Web server restart, abnormal CGI script file terminations, and certificate mismatches.

Field	Description
HTTP/web SSL request log	These are the requests made to the Web servers SSL module. Indicates the pages requested or placed in the secure mode.
HTTP/web access log	HTTP/Web access log.
Communication Manager Restart log	The log contains the last 16 restarts of the server restart, including the level of the restarts, the reason for restart requests, and whether there were escalations for the restarts.
Select a View (selecting multiple Views can give odd results)	
IP events (interfaces up/down; telephone/endpoint registration/unregistration)	The server posts these events through Messaging. For **IF_UP/IF_DOWN**, the system displays the following fields: • board: The board that is in-service or out-of-service, such as the port network, carrier, and slot or PROCR for the control processor IP interface. • IP: The IP address of the interface. • net:_reg: The network region in which the interface resides. • type: The types of interface. • PROCR: Control Processor IP Interface. • C-LAN: Control LAN circuit pack. • MEDPRO: Media Processor circuit pack. • VAL: Voice Announcement over the LAN circuit pack.
Platform bash command history log	The log lists the commands run by interactive bash cells. These commands include: • **`PPID`**: The process ID of the parent shell. • **`PID`**: The process ID of the shell. • **`UID`**: The user ID for which the shell is running. Zero (0) means root or super user.
Linux kernel debug messages	The messages include debug information about the driver, disk, hardware, and memory.
Linux scheduled task log (CRON)	The log displays information from the Linux scheduling daemon.
Communication Manager's hardware error and alarm events	The events that go into the Messaging hardware error and alarm logs.

Field	Description
Communication Manager's software events	The events that go into the Messaging software error log that needs special deciphering by an external tool.
System update/patch event	The update tool events include the following information: • Type of the update tool script used for a particular update file. • Additional information about certain update tool scripts indicating if a process stopped and restarted. • Status of the update tool indicating if the update tool ran successfully.
Communication Manager's denial events	Displays the denial events on the system. These events are not software errors, but unexpected events caused by mismatched translation, mismatched provisioning, network problems, invalid operation, and resource exhaustion.
Select Event Range	The options are: • Today • Yesterday • View entries for this date and time: Enter date in the MM-DD-YYYY format. Enter time in the HH:MM format.
Match Pattern	To limit your search, enter a keyword. For example, a name or message type.
Display Format	Select the display options: • In the **Number of Lines** field, enter the number of lines you want to view at one time. • To view the most recent text line, select **Newest First**. • To view the text without header, select **Remove Header**.

System log results

When you click **View Log** on the System Logs Web page, the results you see vary depending on which of the following logs you chose.

Logmanager debug trace log

Results for the logmanager debug trace log use the following format:

yyyymmdd:*hhmmss[milliseconds]*:*sequence number*:*process name (process ID)*:*priority*:*message*

For example,`20020628:162547538:100:LIC(13648):HIGH:[...license server initializing...]`

In this example,

- *20020628* is the date.
- *162547538* is the time, that is, 16 hours, 25 minutes, 47 seconds, and 538 milliseconds.
- *100* is the sequence number.
- *LIC(13648)* is the process name, followed by the process ID in parentheses.
- *HIGH* is the priority.
- *...license server initializing...* is the message, truncated to save space in the log.

Linux syslog

Results for the Linux system log (syslog) use the following format:

yyyymmdd:*hhmmss.milliseconds*:*sequence number*:*message type*:*priority*:*[machine name] [process name]*:*message*

For example, `20021104:112113.000:12:lxsys:MED:pcct2 ypbind[3196]: broadcast: RPC: Timed out.`

In this example,

- *20021104* is the date.
- *112113.000* is the time, that is, 11 hours, 21 minutes, 13 seconds, and 000 milliseconds.
- *12* is the sequence number.
- *lxsys* is the message type.
- *MED* is the priority.
- *pcct2 ypbind[3196]* is the machine name, pcct2, followed by the process name, ypbind[3196].
- `broadcast: RPC: Timed out` is the message.

Linux access security log

Results for the Linux access security log use the following format:

yyyymmdd:*hhmmss.milliseconds*:*sequence number*:*message type*:*priority*:*server name*:*application name[process ID]*:*description*

For example, `20020102:115000.000:2066:lxsec:MED:myserver PAM_pwdb[29937]: (rsh) session opened for user xyz_login by (uid=25)`

In this example,

- *20020102* is the date.
- *115000.000* is the time, that is, 11 hours, 50 minutes, 00 seconds, and 000 milliseconds.

- *2066* is the sequence number.
- *lxsec* is the message type.
- *MED* is the priority of the message.
- *myserver* is the server from which the system generated the log.
- PAM*_pwdb[29937]* is the application that logged the message, followed by the process ID, pwdb[29937].
- (rsh) session opened for user xyz_login by (uid=25) is the description of the process.

Linux login/logout/reboot log

Results for the Linux login/logout/reboot log use the following format:

yyyymmdd:*hhmmss.milliseconds*:*sequence number*:*message type*:*priority*:*message*

For example, `20021101:170800.000:1:lxwtmp:MED:doejohn pts/1 dura-srv.mycompany.com - 17:08 (08:43)`

In this example,

- *20021101* is the date.
- *170800.000* is the time, that is, 17 hours, 08 minutes, 00 seconds, and 000 milliseconds.
- *1* is the sequence number.
- *lxwtmp* is the message type.
- *MED* is the priority.
- *doejohn* is the user ID of the person who logged in.
- `pts/1 dura-srv.mycompany.com` is the port, pts/1, and machine or PC, dura-srv.mycompany.com from which the user logged in. Instead of the host name, the logs might display the IP address.
- `17:08 (08:43)` is the time the user logged in and the amount of time the user was logged into the system (08:43). If the user is still logged in, the log shows **still logged in**.

Linux file transfer log

Results for the Linux file transfer log use the following format:

yyyymmdd:*sequence number*:*hhmmss.milliseconds*:*transfer time*:*remote host name*:*file size*:*file name*:*transfer type*:*special action taken*:*direction of transfer*:*login method*:*local user name*:*name of service invoked*:*user ID*:*transfer status*

For example,

```
20020114:1:090716.000::MED:rem.servername.com 8143046 /var/home/ftp/
file 1

b _ o a smith@mycompany.com ftp 0 * c
```

In this example,

- *20020114* is the date the ftp transfer took place.
- *1* is the sequence number.
- *090716.000* is the time the FTP transfer took place, that is, 09 hours, 07 minutes, 16 seconds, and 000 milliseconds.
- *::* means the field is unused.
- *MED* is the priority.
- *rem.servername.com* is the remote host name. Instead of the host name, the logs might display the IP address.
- *8143046* is the size of the transferred file in bytes.
- */var/home/ftp/file 1* is the name of the transferred file.
- *b* is the type of transfer. *b* refers to a binary transfer and *a* refers to an ASCII transfer.
- _ is the special action taken. In this case, “” indicates that no action was taken.
- *o* is the direction of the transfer. *o* means that the transfer was outgoing and *I* means that the transfer was incoming.
- *a* is the method by which the user logged in. In this case, *a* means the user logged in using an anonymous login.
- *smith@mycompany.com* is the local user name. If the user logged in using an anonymous or guest login, this field contains the ID string provided when the password was entered, usually an email address.
- `ftp` (file transfer protocol) is the name of the invoked service.

Note:

The system records data in a log file when invoking an FTP session from a remote PC to the host server using an anonymous login. Conversely, the system does not record data in a log file when invoking an FTP session from the host server to a remote PC.

- *0* is the method of authentication used. *0* means that no authentication method was used.
- * is the user ID returned by the authentication method. * indicates that an authenticated user ID is unavailable.
- *c* is the status of the transfer. *c* means the transfer was complete, and an *I* means the transfer was incomplete.

Watchdog logs

Results for the watchdog logs use the following format:

yyyymmdd:*hhmmss.milliseconds*:*sequence number*:*message type*:*priority*:*message*

For example, `20020521:164138.928:5:WATCHD:HIGH:INFO: no hardware watchdog device:/dev/hwsan`

In this example,

- *20020521* is the date when the command was issued.
- *164138.928* is the time, that is, 16 hours, 41 minutes, 38 seconds, 928 milliseconds.
- *5* is the sequence number.
- *WATCHD* is the message type.
- *HIGH* is the priority.
- *INFO: no hardware watchdog device:/dev/hwsan* is the message.

Platform command history log

Results for the Platform command history log use the following format:

month date time [server name] user: *command issued*

For example,

```
20021023:020500.000:721:cmds:MED:baccarat1 root:
/opt/ecs/sbin/filesync -st all
```

In this example,

- *20021023* is the date.
- *020500.000* is the time you issued the server command.
- *721* is the system-generated numbering sequence.
- *cmds* is the command history log
- *MED* is the priority of the session.
- *baccarat1* is the server name.
- *Root* is the user who initiated the command.
- `/opt/ecs/sbin/filesync` **`-st all`** is the command issued by the user.

Storage server logs

Storage server logs overview

Storage server logs are of the following types:

- **Administration History log**: Identifies administrative events that occur on the system. These events include information about any changes to the system, such as logons, command line entries, reports, or changes to software.
- **Administrator's Log**: Identifies system events. These events include problems that you need to correct. Some events such as full user mailboxes and undeliverable messages directly affect message processing.
- **Alarm Log**: Lists active or resolved system alarms. The system lists the most severe alarms first since these are often the cause of the problem.
- **Software Management Logs**: Includes information about the installation, update, and deletion of software packages.
- **Maintenance Log**: Includes descriptions of all reported maintenance events.
- **IMAP/SMTP Messaging log**: Includes information about the status of each email process.
- **Enhanced-List Delivery Failure Log**: Provides information on failed ELA deliveries.
- **User Activity Log**: Tracks a specific user activity by extension and time. You can often resolve reported problems by observing the Activity Log before filing a trouble report.

Viewing the administration history log

About this task

The Administration 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, or changes to software.

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **Administration History**.
2. On the Administration History Log Web page, complete all the fields.
3. Click **Display** to generate the report.

Comments? infodev@avaya.com

The system displays the administration history log.

Administration History Log field descriptions

Field Name	Description
Start Date	The start date for generating the logs. If you leave the field blank, the system displays all qualifying logs. The default value is the date when you last used the page.
Time	The start time for generating the logs. The **Start Date** field must have valid entries before you can use this field. If the **Time** field is blank, the system displays all alarms for the specified start date.
Application	The two-character application code for the administration log entry: • **All**. All applications • **EL**. Enhanced-List Application • **IM**. Internet Messaging • **LD**. LDAP • **MG**: Messaging • **MT**. Maintenance • **SM**. Station Manager • **VM**. Messaging • **VP**. Voice Platform
Search String	A text string that you want the system to search in the administrators log entries. The system searches the **Message** field of the administrators log for matching text.

Administration History Log Results field descriptions

Field	Description
Date	The date the system generated the logs.

Field	Description
Time	The time the system generated the logs.
App	The application code for the administration log entry.
EventID	The event ID for a specific event. A blank field indicates all event types.
Cnt	The count of logs.
Message	The log message.

Viewing the administrators log

About this task

The system warns you of potential administrative problems by displaying an administrative alert message `Alarms: A` on the administration status line when the system logs an administration event. Check the status line at the top of the command prompt screen at least once a day. If you observe such a message, see the Administrators Log to view current error messages and a description for each problem.

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **Administrator**.
2. Enter the appropriate information in the fields.
3. Click **Display**.
   The system displays the administrators log.

Administrator's Log field descriptions

Field Name	Description
Start Date	The start date of the log report. If you leave this field blank, the system displays all logs. The default value is the date when you last used this page.
Time	The start time of the log report. The **Start Date** field must have a valid entry before you can use this field. If the **Time** field is blank, the system displays all alarms for the specified start date.

Field Name	Description
Application	The two-character application code for the administration log entry. Select a value from the drop-down list. • **All**: All applications • **EL**: Enhanced List Application • **IM**: Internet Messaging • **LD**: LDAP • **MG**: Messaging • **MT**: Maintenance • **SM**: Station Manager • **VM**: Messaging • **VP**: Voice Platform
Event ID	The event ID of a specific event. A blank field indicates all event types.
Search String	A text string that you want the system to search in the administrators log entries. The system searches the **Message** field of the administrators log for matching text.

Administrator's Log Results field descriptions

Field	Description
Date	The date the system generated the logs.
Time	The time the system generated the logs.
App	The application code for the administration log entry.
EventID	The event ID for a specific event. A blank field indicates all event types.
Cnt	The count of logs.
Message	The log message.

Viewing the alarm logs

About this task

The alarm logs include descriptions of all significant problems that the system detected including active alarms and resolved alarms. Resolved alarms include those alarms that the system corrects automatically or by implementing diagnostic procedures.

Important:

You must check the alarm logs on a daily basis.

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **Alarm**.
2. Enter the appropriate information in the fields.
3. Click **Display**.
   The system displays the alarm logs.

Alarm Log field descriptions

Field Name	Description
Alarm Type	The options to display the type of alarms include: • **Active** • **Resolved**
Alarm Level: Major	The options to display the major alarms include: • **yes** • **no**
Alarm Level: Minor	The options to display the minor alarms include: • **yes** • **no**

Field Name	Description
Alarm Level: Warning	The options to display the warning alarms include: • **yes** • **no**
Start Date	The start date for generating the logs must be in the MMDDYY format. For active alarms, the date indicates when the system raised the alarms. For resolved alarms, the date indicates when the system resolved the alarms.
Time	The start time for generating the logs must be in the HHMMSS format. If you do not specify the time, the time starts from the beginning of the day, indicated as 00:00:00, for the specified date. If you specify only the time, the start date is the current day. For resolved alarms, the time indicates when the system resolved the alarms.
Application	The two-character application ID that the system uses to identify each module in the system. The system displays log entries with only the specified application ID. You can select any of the following IDs from the drop-down list: • **ALL**: All applications • **EL**: Enhanced-List Application • **IM**: Internet Messaging • **LD**: LDAP • **MG**: Messaging • **MT**: Maintenance • **SM**: Station Manager • **VM**: Messaging • **VP**: Voice Platform
Resource Type	The resource type of the generic alarm that requires maintenance action. The system displays log entries only for the resource type of the specified alarm.

Field Name	Description
Alarm Code	The alarm code that identifies the reason for the alarm against the specific resource.

Alarm Log Results field descriptions

Field Name	Description
App	The two-character application ID that the system uses to identify each module in the system.
Resource Type	The resource type of the generic alarm that requires maintenance action.
Location	The location of the log.
Alarm Code	The alarm code that identifies the reason for the alarm against the specific resource. For detailed information on the alarm codes, see *Avaya Aura® Messaging Alarms and Events*.
Alarm Lvl	The alarm level.
Ack	The indication of whether the administrator has acknowledged the alarm.
Alarmed Date	The date on which the system generated the alarm.
Time	The time at which the system generated the alarm.
Resolved Date	The date on which the system resolved the alarm.
Time	The time at which the system resolved the alarm.
Resolved Reason	The reason for resolving the alarm.

Related topics:

Alarm Log field descriptions on page 256

Viewing the software management logs

About this task

The Software Management Logs Web page displays information on software installation, update, and deletion.

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **Software Management**.
2. Select a log to view from the **Select log to view** drop-down list.

Software Management Logs field descriptions

Field Name	Description
Installation/Removal Log	A log of the most recent software installation, update, or deletion.
Old Installation/Removal Log	A cumulative log of old software installation, update, and deletion sessions. The system displays old sessions in the log beginning with the most recent old session. When a new session begins, the system moves the most recent installation, update, or deletion session log to the beginning of this log.
Summary of Installation/ Removal of Packages	A cumulative, detailed log of software package component installation and deletion attempts. The system records the success or failure of each attempt for each set and set member.

Viewing the maintenance logs

You can view the descriptions of all reported maintenance events on the Maintenance Log Web page.

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **Maintenance**.
2. Enter the appropriate information in the fields.

3. Click **Display**.
   The system displays the maintenance logs.

Maintenance Log field descriptions

Field Name	Description
Errors	Displays the log entries with the event type ERR.
Resolutions	Displays the log entries with the event type RES.
Events	Displays the log entries with the event type EVN.
Start Date	Indicates the start date for generating the logs. The system displays the logs from the specified date. The start date should be in the MMDDYY format.
Time	Indicates the start time for generating the logs. The system displays the logs generated from the specified time. If you do not specify the time, the system considers time of the day indicated as 00:00:00 as the start time. If you specify only the time, the current day is used as the start date.
Application	The two-character application code for the administration log entry: • **All**. All applications • **EL**. Enhanced-List Application • **IM**. Internet Messaging • **LD**. LDAP • **MG**: Messaging • **MT**. Maintenance • **SM**. Station Manager • **VM**. Messaging • **VP**. Voice Platform
Event ID	Identifies the reported event. The system displays the log entries with the specified Event ID code.
Problem Resource Type	Identifies the logical resource type or reported system component. The system displays the log entries with the specified problem resource type.

Field Name	Description
Reporting Resource Type	Identifies the logical resource type of the resource that discovers and detects the problem. The system displays the log entries with the specified reporting resource type.
Reporting Resource Source	Identifies the specific line of code reporting the condition. The system displays the log entries with the unique value used to display the specified reporting resource source.
Search String	The system displays the log entries that include the specified text entries.

Maintenance Log Results field descriptions

Name	Description
Problem Resource Type	Indicates the logical resource type or reported system component. The system displays log entries with the specified problem resource type.
Inst	The event ID.
Location	The location of the log.
Msg Type	The event type.
Report Resource Type	Identifies the logical resource type of the resource that discovers and detects the problem. The system displays log entries with the specified reporting resource type.
Inst	The event ID
Resource	The resource.

Viewing the Internet messaging logs

About this task

The Internet messaging logs include information about occurrences at each stage in the messaging process..

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **IMAP/SMTP Messaging**.
2. In the **Select log to view** drop-down list, select a type of log to view.
3. To clear the logs from the page, click **Clear the Log**.

Internet Messaging Logs field descriptions

Field Name	Description
User Agent Log	Software interfaces called delivery agents are required for the message transport agent (MTA) to function with the user agent (UA).
Remote Delivery Agent Log	Accepts messages from the User Agent through the Outbound queue and delivers these messages to the Queuer.
Local Delivery Agent Log	Accepts messages from the MTA through the Dispatcher. Passes incoming messages to the UA through the Inbound queue.
Queuer Log	Accepts messages from the RDA and passes these messages to SMTP Out or stores these messages in the SMTP queue until the system accepts these messages.
Dispatcher Log	Accepts messages from SMTP In and passes these messages to the LDA, or stores these messages in the SMTP queue until the system accepts these messages.
SMTP In Log	Transfers incoming messages from the Internet to the Dispatcher.
SMTP Out Log	Transfers outgoing messages from the Queuer to the Internet.
Administration/Event Log	Records occurrences that are informational or require administrator intervention.
IMPAP4 Log	Records errors and events occurred in the communication between POP3 and IMAP4 clients of the user and the message server. Additional information includes errors and significant events dealing with the server and the rest of the Messaging system.
IMAP4/POP3 Access Log	Records data about every login attempt and every logout. The log includes data for IMAP4 super-user bind and unbind along with the login success or failure and the

Field Name	Description
	reason. Additional information includes the Far-end IP address and port, mailbox-number, and time.

Viewing the ELA delivery failure logs

About this task

The Enhanced-List Delivery Failure Log Web page provides information on failed ELA deliveries.

Procedure

On the **Administration** menu, click **Messaging** > **Logs** > **ELA Delivery Failures**.

Enhanced-List Delivery Failure Log field descriptions

Field Name	Description
Date	The date of failure delivery.
Time	The time of failure delivery.
Message Originator	The mailbox number of the originator of the failed message.
Parent List	The enhanced list to which the originator sent the message. The Parent List can be a local or remote list mailbox.
Child List	The last enhanced list visited in a nested enhanced list hierarchy before the message failed. The Child List is a local mailbox. If the enhanced lists are not nested, the Child List is the same as the Parent List.
Failed Recipient	The name of the intended recipient of the failed message.
Failed Address	The mailbox number of the intended recipient of the failed message. The Failed Address can be the system broadcast mailbox.
Failure Reason	The detailed reason for the delivery failure.

User activity logs

The user activity log is an administrative tool used for investigating problems reported for message delivery and the operation of MWI. The activity log maintains a history of the activity on the Messaging system.

You can use the log to track the activity of a user using the mailbox number and time. You can resolve reported problems by observing the activity log before filing a trouble report.

Configuring a user activity log

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Activity Log Configuration**.
2. Enter the appropriate information in the fields.
3. Click **Save**.
   The system saves the details.

User Activity Log Configuration field descriptions

Name	Description
Activity Log Enabled	Indicates if the user activity is enabled or disabled.
Maximum Number of Activity Log Entries	Indicates the maximum number of activity log records.
Clear All Entries in Activity Log	Indicates if you want to clear all entries in the activity log.

Running an activity log report

Note:

The report can take several minutes to run depending on the system load and the size of the log file.

Comments? infodev@avaya.com

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **User Activity**.
2. Enter the mailbox number of a user on the system.
3. Select the duration from the **Start Date** and **End Date** fields for which you want to view the user activity.
4. Click **Display**.
   The system displays the activity log.

User Activity Log field descriptions

Field Name	Description
Mailbox Number	The mailbox number of a user on the system.
Start Date	The start date for generating logs. The system displays the log entries for the specified date and forward.
End Date	The end date for generating logs. The system displays the log entries up to the specified date.
Time	The time in hours and minutes for generating the logs.
User Activity Log Results	
Name	The name of the user.
Mailbox Number	The mailbox number of the user.
Date	The log date.
Time	The log time.
Activity	The user activity.
Description	The description of the user activity. The id number is the last five digits of a unique number that identifies a specific imapd session. The system assigns the id number with each new IMAP4 connection and retires the id number when the connection ends. If you want to trace a problem with a session of an Aria user, you can map the id number in User Activity Log to the full number in IMAP4/POP3 Access Log. The session id is the field just before the field containing *On* or *Off* in IMAP4/POP3 Access Log.

Application server logs

Application server logs overview

The application server has the following logs:

- System Log Filter: Provides you access to the full system log with advanced filtering options to zoom specific constraints. All displayed times reflect the time zone of the application server.
- Call Records: Displays all incoming and outgoing phone activities on the application server. All displayed times reflect the time zone of the application server. The system rotates current phone logs on a monthly basis. The Current Log section displays the phone log for the current month.
- Reporting Logs: There are two types of reporting logs:
  - Audit Log: The audit log is a historical log of application server cluster configurations. The audit log tracks all configuration changes made to the system. All displayed times reflect the time zone of the application server. The details of the audit log include the date and time of change, the changed object, and the new value.
  - Port Usage Logs: The system creates and saves the Port Usage logs daily on the application server in comma-separated value (.csv) format. All displayed times reflect the time zone of the application server.
- Diagnostics Results: The application server diagnostics generates these results. All diagnostics results for a given day are stored in a single log file. The system deletes the diagnostics log files from the application server after 14 days.
- Call Logs: The call logs provide traces of individual calls for application tuning.

Configuring the log settings

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **Log Configuration**.
2. In the **System logging mode** area, select the logging option.

   By default, the system sets the mode to **Normal**. If you want to test the configuration, you can temporarily select **Testing** for more detailed logging.

Comments? infodev@avaya.com

For detailed troubleshooting, select **Debug** or **Extensive**. You must select these logging modes only when advised by qualified support personnel. These logging modes generate logging data that could affect system performance.

3. Click **Apply**.
   The system displays a confirmation dialog.
4. Click **OK** to proceed.

Log Configuration field descriptions

Name	Description
System logging mode	The options are: • Normal • Testing • Debug • Extensive By default, the system sets the mode to Normal. If you want to test the configuration, you can temporarily select Testing for more detailed logging. For detailed troubleshooting, select Debug or Extensive. You must select these logging modes only when advised by qualified support personnel. These logging modes generate logging data that could affect system performance.

Running the system log filter

The System Log Filter Web page provides you access to the full system log. Use the advanced filtering options at the time of generating logs.

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **System Log Filter**.
2. Enter the appropriate information in the fields.
3. Click **View**.
   The system displays the log messages.

System Log Filter field descriptions

Field	Description
Date Interval	The **Date Interval** drop-down list changes the date interval for the log filter. The options are: • The default value is **Last Day**. The log filter displays all events for the last day. • **Specific** defines a specific interval in the **Start Date** and **End Date** fields. • **All** does not filter logs by date.
Category	The system component using which you can filter the system log. The options are: • **All** • **Voice Browser** • **Infobridge** • **Health Monitor** • **Cache** • **Configuration** • **Hardware** • **Telephony Integration Summary** • **Telephony Integration Details** • **Exchange Integration**
Severity	The severity level to filter the system log. The options are: • **All** • **Err** • **Warning** • **Notice** • **Info** • **Debug**
Phone Line (optional)	The affected phone line to filter the system log.
Session ID (optional)	The Session ID to filter the system log.

Field	Description
Tag (optional)	This field is currently unused.
Number of lines in log to filter (optional)	The number of lines in the log to which the system applies the filter.

Note:

Filtering based on Phone Line, Session ID, and Tag is only relevant for certain log events that qualified support personnel generally use.

Collecting the system log files

Use this page to download log files for the application server system. You can download the log files for the last hour or for a time duration that is specific.

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **Collect System Log Files**.
2. For **Date Interval**, select one of the following:
   - **Last Hour**
   - **Specific** and provide **Start date**, **End date**, and **Time**
3. Click **Download**.
   The system prompts you to download the zipped log file.
4. Save the system log file to a location of your choice.

Collect System Log Files field descriptions

Name	Description
Date Interval	Select one of the following: • Last Hour • Specific and provide Start date, End date, and Time

Viewing the call records

Use the Call Records Web page to view the call records of all incoming and outgoing calls on the application server. All displayed times reflect the time zone of the server. The system

rotates current call records on a monthly basis. The **Current Log** section shows the call records for the current month.

The system displays the phone logs call record in XML format with LOG_ENTRY entries for each call record.

Note:

For an incoming call that also generates an outgoing call, the system logs the outgoing call record before the incoming call record.

Procedure

On the **Administration** menu, click **Messaging** > **Logs** > **Call Records**.
The system displays the current log.

Accessing audit and ports usage files

The audit log is a historical log of cluster configurations. The audit log tracks all configuration changes made to the system over a period. All displayed times reflect the time zone of the application server. The details of the audit log include the date and time of the change, the changed object, and the new value to be assigned.

The system creates and saves port usage logs daily on the application server in the comma-separated value (.csv) format. You can save the log files in your machine and then use the files.

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **Audit/Ports Usage**.
2. Select one of the following:
   - To access the audit log, click `configd-audit.log`.
   - To access a port usage log, click the port usage log (.csv) file that you want to view.
3. Save the file on your system.

   The best way to view the audit log is using a structured text editor, for example, TextPad or WordPad.

   You can view the port usage log using the port usage template. For more information, see Viewing the port usage report on page 271.

Viewing the port usage report

Before you begin

Enable macros in Microsoft Office.

Procedure

1. Download the port usage log to your system. For more information, see Accessing audit and ports usage files on page 270.
2. To create reports and graphs from the port usage log, click the link to download the template.
3. Save the template on your system.
4. Open the template file.
   The system displays a dialog to create the port usage report.
5. Click **OK**.
6. Select the port usage log that you downloaded in Step 1 and click **OK**.
   The port usage report replaces the content in the ports usage log with tables and graphs.
   For more information, see Port Usage Report descriptions on page 271.

Port Usage Report descriptions

Worksheet	Description
Chart_Max_Usage	The chart displays the maximum number of ports used at every hour.
Chart_100_Percent_Port_Usage	The chart displays whether the system uses 100% of the ports at every hour..
Chart_50_Percent_Port_Usage	The chart displays whether the system uses 50% of the ports at every hour.
Chart_Activations_By_Port	The chart displays the activations by port.
Data	The sheet displays the following details: • Start Date: The start date on the application server in local time. • Start Time: The start time on the application server in local time. • End Date: The end date on the application server in local time.

Worksheet	Description
	• End Time: The end time on the application server in local time. • Seconds: The period in seconds. • Outbound Alloc Failures: The number of attempts to allocate a line for outbound calls that failed due to lines being unavailable. • MWI Alloc Failures: The number of attempts to allocate a line for MWI usage that failed due to lines being unavailable. • All Ports >= 50% Util: The proportion of time the overall port usage was greater than or equal to 50% of all ports. • All Ports at 100% Util: The proportion of time the overall port usage was equal to 100% of all ports. • Max Ports Used: The maximum number of ports in use over a period. • Inbound Eligible Ports >= 50% Util: The proportion of time the inbound port usage was greater than or equal to 50% of ports eligible for inbound usage. • Inbound Eligible Ports at 100% Util: The proportion of time the inbound port usage was equal to 100% of ports eligible for inbound usage. • Max Inbound Eligible Ports Used: The maximum number of inbound ports in use over a period. • Outbound Eligible Ports >= 50% Util: The proportion of time the outbound port usage was greater than or equal to 50% of ports eligible for outbound usage. • Outbound Eligible Ports at 100% Util: The proportion of time the outbound port usage was equal to 100% of ports eligible for outbound usage. • Max Outbound Eligible Ports Used: The maximum number of outbound ports in use over a period. • MWI Eligible Ports >= 50% Util: The proportion of time the MWI port usage was greater than or equal to 50% of ports eligible for MWI usage. • MWI Eligible Ports at 100% Util: The proportion of time the MWI port usage was equal to 100% of ports eligible for MWI usage. • Max MWI Eligible Ports Used: The maximum number of MWI ports in use over a period. • For each telephony port: - Port #1 Inbound Activations: The number of times the system activated the port for inbound use. - Port #1 Outbound Activations: The number of times the system activated the port for outbound use.

Worksheet	Description
	- Port #1 MWI Activations: The number of times the system activated the port for MWI use. - Port #1 Inbound Seconds Active: The seconds for which the port was active for inbound use. - Port #1 Outbound Seconds Active: The seconds for which the port was active for outbound use. - Port #1 MWI Seconds Active: The seconds for which the port was active for MWI use.
ByPort	The sheet displays the following details for every port: • Inbound Activations: The number of times the port was active for inbound use. • Outbound Activations: The number of times the port was active for outbound use. • MWI Activations: The number of times the port was active for MWI use. • Total Activations: The total number of activations. • Inbound Utilization: The % of inbound port utilization. • Outbound Utilization: The % of outbound port utilization. • MWI Utilization: The % of MWI utilization. • Overall Utilization: The overall utilization.
ByHour	The sheet displays the following details for every hour: • Outbound Port Allocation Failures: : The number of attempts to allocate line for outbound calls that failed due to lines being unavailable. • MWI Port Allocation Failures: The number of attempts to allocate line for MWI usage that failed due to lines being unavailable. • %Time All Port Util >= 50%: The proportion of time the overall port usage was greater than or equal to 50% of all ports. • Time All Port Util = 100%: The proportion of time the overall port usage was equal to 100% of all ports. • Max Ports Used: The maximum number of ports in use over a period. • %Time Inbound Eligible Port Util >= 50%: The proportion of time the inbound port usage was greater than or equal to 50% of ports eligible for inbound usage. • %Time Inbound Eligible Port Util = 100%: : The proportion of the time inbound port usage was equal to 100% of ports eligible for inbound usage.

Worksheet	Description
	• Max Inbound Eligible Ports Used: The maximum number of inbound ports in use over a period. • %Time Outbound Eligible Port Util >= 50%: The proportion of time the outbound port usage was greater than or equal to 50% of ports eligible for outbound usage. • %Time Outbound Eligible Port Util = 100%: The proportion of time the outbound port usage was equal to 100% of ports eligible for outbound usage. • Max Outbound Eligible Ports Used: The maximum number of outbound ports in use over a period. • %Time MWI Eligible Port Util >= 50%: The proportion of time the MWI port usage was greater than or equal to 50% of ports eligible for MWI usage. • %Time MWI Eligible Port Util = 100%: The proportion of time the MWI port usage was equal to 100% of ports eligible for MWI usage. • Max MWI Eligible Ports Used: The maximum number of MWI ports in use over a period.

Accessing diagnostics results

The Diagnostics Results (Application) Web page provides you access to the results generated by the application server diagnostics. Time stamps of the logged files reflect the time zone of the application server. All diagnostics results for a day are stored in a single log file. The system deletes diagnostics log files from the application server after 14 days.

Procedure

1. On the **Administration** menu, click **Messaging** > **Logs** > **Diagnostics Results (Application)**.
   The Diagnostic Results (Application) Web page displays a list of diagnostic logs generated using the **Messaging** > **Diagnostics** > **Diagnostics (Application)** Web page.

   For information on running the diagnostics, see Running application server diagnostics on page 337.
2. To download all diagnostic logs as a zip file, click **Download**.
3. To download a specific diagnostic log, click the particular log.

Sending logs to an external syslog server

Use the Syslog Server Web page to select the logs that the system sends to an external syslog server. The Syslog Server Web page supports both IPv4 and IPv6 network connections.

Note:

The IPv6 network support is limited to a specific customer set and is not for general use.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Syslog Server**.
2. Enter the appropriate information in the fields.
3. Click **Submit**.
   The system saves the changes.

Syslog Server field descriptions

Name	Description
Control File Synchronization of Syslog Configuration	
When the Submit button is clicked, send syslog configuration to all LSP and ESS servers	Select this check box to send the syslog configuration information to the Local Survivable Server (LSP) and Enterprise Survivable Server (ESS) servers when you click **Submit**. • *LSP*: When the main server fails, the LSP server continues to operate independently and manages locally attached resources. • *ESS*: When the main server fails, the ESS server continues to operate independently and manages locally attached resources. However, more importantly the ESS server manages other surviving port networks that the ESS server remains in communication with.
Control Logging to an External Syslog Server	

Name	Description
Disable logging to an external syslog server	Click this option to disable logging to an external syslog server. By default, the system selects this option.
Enable logging to the following syslog server	Click this option to enable logging to the syslog server you specify in the **Specify the Syslog Server to Receive Events** area. The settings on the Syslog Server Web page are saved regardless of whether you select **Disable logging to an external syslog server** or **Enable logging to the following syslog server**.
Specify the Syslog Server to Receive Events	
server name	Enter the address of the syslog server to receive events. The **server name** field can contain up to 40 characters and can either be a URL, for example, www.asite.com or a literal address. For an IPv6 network, the literal address can be a global unicast address, for example, 2002:8709:b5fe:: 75 or a link local address, for example, fe80::2ca:feff:fe03:5053%eth0.
Select Which Logs Are to be Sent to the Above Server	
boot, cron, *.emerg logs	Select this check box to send the boot, cron, and *.emerg logs to the external server.
security log	Select this check box to send the security log to the external server.
kernel log	Select this check box to send the kernel log to the external server.
command history log	Select this check box to send the command history log to the external server.
CM IP events log	Select this check box to send the CM IP events log to the external server.

Chapter 17: Reports

Reports overview

You can use the SMI to generate predefined Messaging reports. These reports are useful for monitoring users, system usage, planning capacity, and tracking system security.

The storage server collects information about system settings and properties. The storage server also collects information that depicts the system use, including data about features, users, communities, data port loads, and remote-messaging traffic. The Messaging system displays this information in real-time dynamic report pages and in the Messaging traffic reports.

Report types

Report	Description
Reports (Storage)	Provides a summary of Users (Local), Information Mailboxes, Remote Users, Uninitialized Users, Login Failures, and Locked Out Users.
System Evaluation Report (Storage)	Provides a summary of various Messaging settings and properties. This report also displays information about dormant mailboxes. A dormant mailbox is a mailbox that a user has not accessed in 30 days or a new mailbox that has not received any messages since 30 days.
Internet Messaging Traffic (Storage)	Provides a summary of the port usage on the Messaging system in daily or hourly periods. Use the report to determine if the Messaging system is performing at peak efficiency by providing the actual usage information. This report also provides information about outcalling ports, user traffic, and feature traffic that helps to evaluate system efficiency.

Report	Description
TCP/IP Snapshot	Provides the total traffic for all machines with the specified connection type. Also displays the total number of updates.
Messaging Measurements	Displays daily measurements of traffic by community, feature, load, network load, and user.

When the Messaging system exhausts all attempts to deliver a voice mail to a user mailbox, the system sends a Non-delivery Report (NDR) or Delivery Status Notification (DSN) to the user. If the user addresses the voice mail to a System Distribution List (SDL), the system sends NDRs also to the postmaster mailbox. The system does not present NDRs to Exchange users.

Viewing the local users report

Procedure

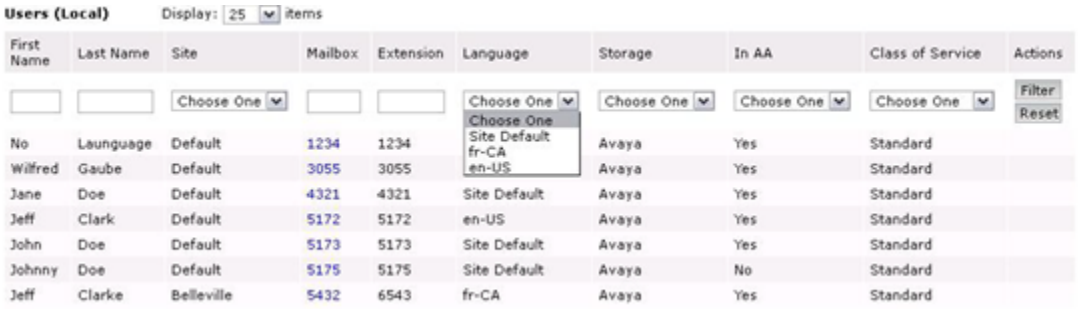
On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.

Tip:

Click on the column header to sort the data.

Example

The following image displays the local users report with the *Language* filter used to sort users.



Users (Local) field descriptions

The report displays a list of local users present in the Messaging system.

Name	Description
Display	Use to control the number of users displayed on a particular page. The options are: • 25 • 50 • 100 • All
First Name	The first name of the user.
Last Name	The last name of the user.
Site	The site to which the user belongs.
Mailbox	The mailbox of the user.
Extension	The user extension.
Language	The language configured for the user. For more information on the language, see Supported languages on page 21.
Storage	The storage option for the user.
In AA	Indicates whether the user belongs to Auto Attendant.
Class of Service	The CoS to which the user belongs.
Actions	Click **Filter** to sort according to the selected option. Click **Reset** to reset all the filters to default.

Viewing the information mailboxes report

Procedure

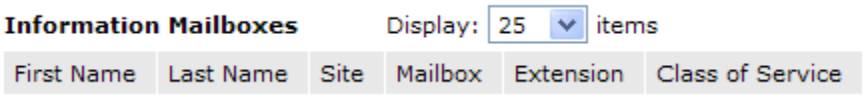
On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Info Mailboxes**.

Tip:

Click on the column header to sort the data.

Example

The following image displays the columns visible in the information mailboxes report.



Information Mailboxes field descriptions

A list of information mailboxes in the Messaging system.

Name	Description
Display	Use to control the number of information mailboxes displayed on a particular page. The options are: • 25 • 50 • 100 • All
First Name	The first name of the information mailbox.
Last Name	The last name of the information mailbox.
Site	The site to which the information mailbox belongs.
Mailbox	The mailbox number of the information mailbox.
Extension	The extension of the information mailbox.
Class of Service	The CoS to which the information mailbox belongs.

Viewing the remote users report

After adding users, you must reload the GAL or wait for the nightly maintenance to view the users. To reload the GAL, see Loading lists on page 175.

Procedure

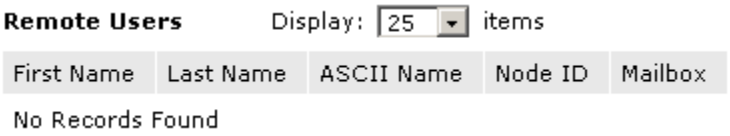
On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Remote Users**.

Tip:

Click on the column header to sort the data.

Example

The following image displays the columns visible in the remote users report.



Remote Users field descriptions

The report displays a list of remote users in the Messaging system.

Name	Description
Display	Used to control the number of users displayed on a particular page. The options are: • 25 • 50 • 100 • All
First Name	The first name of the user.
Last Name	The last name of the user.
ASCII Name	The ASCII name of the user.
Node ID	The node ID of the user. The node ID is the ID you define in the mapping table so that the local system can recognize the remote user.
Mailbox	The mailbox number of the user.

Viewing the uninitialized mailboxes report

Procedure

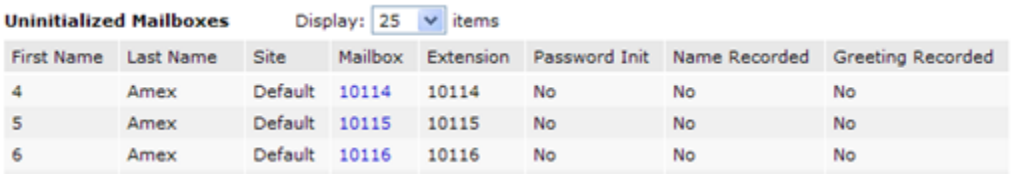
On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Uninitialized Mailboxes**.

Tip:

Click on the column header to sort the data.

Example

The following image displays the columns visible in the uninitialized mailboxes report.



Uninitialized Mailboxes Display: 25 items

First Name	Last Name	Site	Mailbox	Extension	Password Init	Name Recorded	Greeting Recorded
4	Amex	Default	10114	10114	No	No	No
5	Amex	Default	10115	10115	No	No	No
6	Amex	Default	10116	10116	No	No	No

Uninitialized Mailboxes field descriptions

The administrator has enabled users to use voice messaging, but these users have not completed initializing the user mailbox.

Name	Description
Display	Use to control the number of users displayed on a particular page. The options are: • 25 • 50 • 100 • All
First Name	The first name of the user.
Last Name	The last name of the user.
Site	The site to which the user belongs.
Mailbox	The mailbox number of the user.

Name	Description
Extension	The user extension.
Password Init	The administrator provides a new user with a temporary password that the user must change at the first logon through the TUI or the User Preferences page. Users cannot listen to voice messages without logging on to the system and changing the temporary password. The options are: • *Yes*: You must change your password at first logon. • *No*
Name Recorded	The system updates new users to record their names when the users log on to the TUI for the first time. Callers hear the recorded name in the Auto Attendant. The options are: • *Yes*: You must record your name at first logon. • *No*
Greeting Recorded	When users log on to the TUI for the first time, the system updates users to record a personal greeting. The system plays the greeting to callers when the user does not answer the call. The options are: • *Yes*: You must record a personal greeting at first logon. • *No*

Viewing the login failures report

Procedure

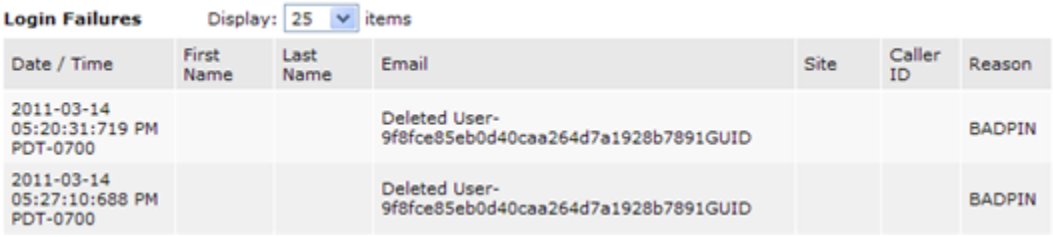
On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Login Failures**.

Tip:

Click on the column header to sort the data.

Example

The following image displays the columns visible in the login failures report.



Login Failures Display: 25 items

Date / Time	First Name	Last Name	Email	Site	Caller ID	Reason
2011-03-14 05:20:31:719 PM PDT-0700			Deleted User-9f8fce85eb0d40caa264d7a1928b7891GUID			BADPIN
2011-03-14 05:27:10:688 PM PDT-0700			Deleted User-9f8fce85eb0d40caa264d7a1928b7891GUID			BADPIN

Login Failures field descriptions

The report displays a list of users with failed login authentication attempts.

Name	Description
Display	Use to control the number of users displayed on a particular page. The options are: • 25 • 50 • 100 • All
Date / Time	The date and time of the failure.
First Name	The first name of the user.
Last Name	The last name of the user.
Email	The email address of the user.
Site	The site to which the user belongs.
Caller ID	The caller ID.
Reason	The reason for the failure.

Viewing the locked out users report

Procedure

On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Locked Out Users**.

Tip:

Click on the column header to sort the data.

Example

The following image displays the columns visible in the locked out users report.



Locked Out Users field descriptions

The system displays a list of users locked out of the Messaging system. To unlock a user on this list, go to the User Properties Web page and clear the **Locked out from voice messaging** check box.

Name	Description
Display	Use to control the number of users displayed on a particular page. The options are: • 25 • 50 • 100 • All
First Name	The first name of the user.
Last Name	The last name of the user.
Site	The site to which the user belongs.
Mailbox	The mailbox number of the user.
Extension	The extension of the user.

Running the system evaluation report

This page displays a summary report of various system settings and properties. Depending on the system, the summary report displays different types of dynamic information.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Reports** > **System Evaluation (Storage)**.

   The system displays the report.

2. To refresh the report, click **Re-run System Report**.

   The System Evaluation Report (Storage) Web page displays the following information:

   - **System Status**
   - **Site Information**
   - **Software Summary**
   - **Hardware Summary**
   - **Reliability Information**
   - **Networked Machines**, if administered
   - **Extension Ranges**
   - **Dormant Mailboxes**
   - **File System Usage**
   - **Installed Software Packages**

Viewing the Internet messaging traffic

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Reports** > **IMAP/SMTP Traffic (Storage)**.

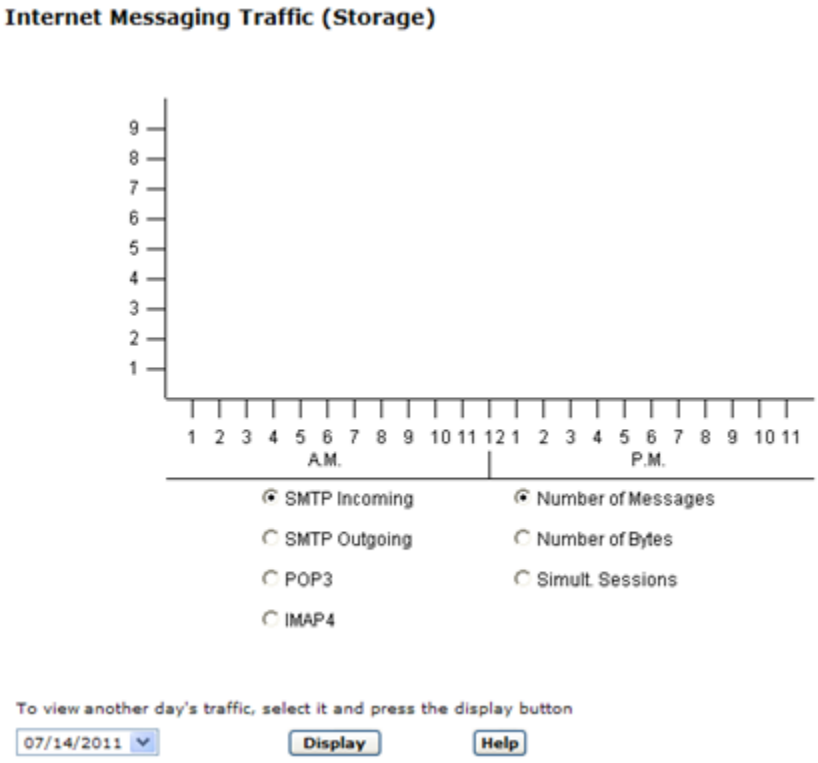
   The system displays a security warning if the system cannot verify the certificate of the website. Click **Yes** to continue.

   The Internet Messaging Traffic (Storage) Web page displays a graph of the traffic for the selected days.

2. Select the options for which you want to view the report.
3. If you want to view the traffic of a different day, select the day from the drop-down list and click **Display**.
   The system displays the report for the selected day.

Example

The following report displays a graph of the traffic for the selected day.



Internet Messaging Traffic field descriptions

Name	Description
X-axis	Use the X-axis to see the following information: • **SMTP Incoming** • **SMTP Outgoing** • **POP3** • **IMAP4**

Name	Description
Y-axis	Use the Y-axis to see the following information: • **Number of Messages** • **Number of Bytes** • **Simult. Sessions** • **Total Sessions** **Note:** **Simult. Sessions** is available with **SMTP Incoming** and **SMTP Outgoing**. **Total Sessions** is available with **POP3** and **IMAP4**.

Viewing the TCP/IP snapshot

This page displays the current status of the network connection.

Procedure

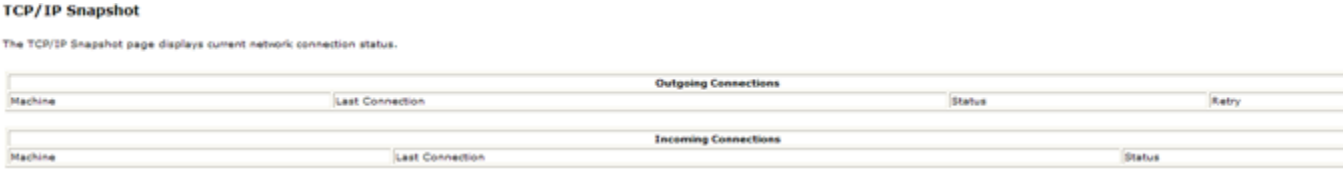
On the **Administration** menu, click **Messaging** > **Server Reports** > **TCP/IP Snapshot**.

The TCP/IP Snapshot Web page displays the status of the incoming and outgoing connection:

- **Machine**
- **Last Connection**
- **Status**
- **Retry**

Example

The following report displays the columns visible in the TCP/IP Snapshot Web page.


TCP/IP Snapshot

The TCP/IP Snapshot page displays current network connection status.

Outgoing Connections			
Machine	Last Connection	Status	Retry

Incoming Connections		
Machine	Last Connection	Status

Running the traffic measurement report

Use the Messaging Measurements Web page to request traffic measurements from the Messaging system.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Reports** > **Measurements (Storage)**.
2. Select the appropriate information.
3. Click **Get Report**.
   The system displays the report.

Example

The following image shows the columns visible in the community traffic measurements report.



Messaging Measurements field descriptions

Name	Description
Type	The types of traffic include: • **Community**: The traffic information for community users. • **Feature**: The traffic information for Messaging features. • **Load**: The traffic information for user thresholds and voice ports.

Name	Description
	• **Network-Load**: The traffic information for network measurements and port usage. • **Subscriber**: The traffic information for a user.
Cycle	Indicates the frequency type to sample. The traffic type determines the frequency types you can select. The frequencies that are available for selection are hourly or daily.
Start Date	The date to start sampling.
Mailbox Number	The system displays this field only when you select the **Subscriber** type. The mailbox number of the user.

Viewing the login reports

Use the Login Reports Web page to generate reports for local host logins administered on this server. You can generate the reports for all local host logins or for an individual local host login.

The system maintains the credentials of local host logins on the server. If you are using an external Authentication, Authorization and Accounting (AAA) server, the system maintains the credentials for those logins on the external AAA server and you cannot view the credentials from this page.

Note:

Your login might not have permission to view all the data for a particular login. If this is the case, the page will display `access denied` for that information.

Procedure

1. On the **Administration** menu, click **Server Maintenance** > **Security** > **Login Reports**.
2. Select an option for the type of login report you want to view.
3. In the **Enter Time Period for Reports** area, enter the time period details.
4. In the **Output Format** area, enter the appropriate details.
5. Click **Continue** to generate the report.

The system displays the login report for the selected type.

Login Reports field descriptions

Name	Description
Select an option	
List Local Host Logins	Select this option to generate a report for all local host logins.
Display Information for Local Host Login	Select this option and enter the individual login name to generate a report for the individual local host login.
Display Information for Failed Logins	Select this option to generate a report of failed logins.
Display Information for Successful Logins	Select this option to generate a report of successful logins.
Display Detailed Information for Successful Logins	Select this option to generate a detailed report for the successful logins. The default *all* keyword will generate a report that includes all successful logins. If you need detailed information on a specific login, replace the keyword *all* with the specific login. The system generates a detailed report for the specific login.
Enter Time Period for Reports	
Start Day/Time	Enter the start time for the report in the format mm:dd and hh:mm.
End Day/Time	Enter the end time for the report in the format mm:dd and hh:mm.
Output Format	
Enter Maximum Number of Lines to Display	Enter the maximum number of lines to display. The default value is 200.
Display Reports Newest First	Select this check box if you want the system to display the newest reports first.

Chapter 18: Maintenance

Maintenance checklist

The following tables list the tasks that you must complete on a regular basis to ensure that the Messaging system operates properly. The first table lists the maintenance tasks for the application server. The second table lists the maintenance tasks for the storage server.

Note:

If you need technical support, locate your product ID before you contact your remote support center. The product ID is a 10-digit number that the support center uses to identify your Messaging server. You can locate your product ID by clicking on the **Administration** menu, and then clicking **Server (Maintenance)** > **Alarms** > **Current Alarms**.

Related topics:

Application server on page 293
Storage server on page 295

Application server

Number	Tasks	Links	Frequency
1	Check the port usage report.	For more information, see: • Accessing audit and ports usage files on page 270 • Viewing the port usage report on page 271	Daily.
2	Check the alarm log. The log displays active alarms and resolved alarms.	For more information, see: • Logs overview on page 243 • Viewing the alarm logs on page 256	Daily.

Number	Tasks	Links	Frequency
3	Check the system logs. Use the log to diagnose network problems, security issues, system reboots, and so on.	For more information, see: • Logs overview on page 243 • Viewing the system logs on page 244	Daily.
4	Follow IT processes for: • Security procedures for virus scans • Critical updates • Windows backups • Defragmentation (defrag) • Check disk (chkdsk) • Scan disk (scandisk) Obtain the recommended schedule for these tasks from your customer IT representative. Analyze the disk before running the *Defragment* command. **Note:** The Microsoft guideline is to perform the tasks once a week.	For more information, contact your customer IT representative.	As required by internal IT standards. Perform the Disk Defragmenter: • During off-peak times. • After a major change to the application software. • After the addition of many files. • When a maintenance alarm in the software instructs you to run the defragment command.
5	Back up the data.	For more information, see: • Back up and restore overview on page 211 • Backing up application files on page 72	Nightly according to the routine automatic schedule. Perform the backup task as necessary: • After making major system changes. • After creating new users. • When experiencing system problems to avoid losing

Number	Tasks	Links	Frequency
			information entered since the last backup. • When a partial backup occurs to avoid losing the data sets that the system did not back up.
6	Verify that the backup completed successfully.	For more information, see Viewing backup logs on page 220.	Daily.
7	Restore the data.	For more information, see: • Back up and restore overview on page 211 • Performing a restore on page 221	Perform the restore task as necessary: • If the application server data is lost or corrupted. • If the system fails because of data loss. • If the hard disk fails.
8	Check for available service packs to download from the Avaya Support website at http://www.avaya.com/support. .		Monthly.
9	Reboot the application server.	For more information see, Shutting down the server on page 373.	As necessary or once a year.

Storage server

Number	Tasks	Links	Frequency
1	Check the events to identify routine conditions and conditions that can lead to a storage server alarm.	For more information, see the *Avaya Aura® Messaging Alarms and Events* document.	Daily.

Number	Tasks	Links	Frequency
2	Administer and check the user activity log. Use the log to investigate user activity and to resolve reported problems.	For more information, see: • Storage server logs overview on page 252 • User activity logs on page 264 • Configuring a user activity log on page 264 • Running an activity log report on page 264	Daily.
3	Check the alarm log. The log displays active alarms and resolved alarms.	For more information, see: • Storage server logs overview on page 252 • Viewing the alarm logs on page 256	Daily.
4	Check the administration log. Use the log to review and investigate administrative entries that you can solve.	For more information, see: • Storage server logs overview on page 252 • Viewing the administration history log on page 252 • Viewing the administrators log on page 254	Daily.
5	Check the backup log. Use the log to identify errors that occurred during the backup.	For more information, see: • Viewing backup history on page 220 • Viewing backup logs on page 220	Daily.
6	Reset the local user password if the user forgets the user password.	For more information, see Resetting the voice mailbox password on page 150.	As necessary.

Number	Tasks	Links	Frequency
7	Unlock a voice mailbox account. Messaging automatically locks the system when the user fails to enter proper login credentials after a certain number of consecutive failed attempts. The **Lock out users after** field on the System Policies Web page determines the number of allowable consecutive failed attempts. The user cannot access the system until an administrator unlocks the user mailbox. Before you unlock a user mailbox, investigate why the system locked the mailbox.	For more information, see: • Unlocking the voice mailbox account on page 149 • Viewing the locked out users report on page 285	As necessary.
8	Reboot the storage server.	For more information see, Shutting down the server on page 373.	As necessary or once a year.
9	Check the Linux system clock.	For more information, see Verifying the system clock on page 38.	Monthly and when a daylight saving time change occurs.
10	Add, delete, or modify local users to maintain user profiles that reflect current needs and staffing.	For more information on how to manage local users, see: • Adding users on page 134 • Adding users from Active Directory on page 135 • Changing user properties on page 136 • Deleting users on page 137 • Viewing the local users report on page 278	As necessary.

Number	Tasks	Links	Frequency
11	Administer remote users. A remote update can use one of your networking ports for quite some time. Administer a user manually when you want to administer a remote user immediately, but do not want to run a remote update.	For more information, see: • Remote updates on page 152 • Running a remote update manually on page 153 • Viewing the remote users report on page 280	As necessary.
12	Check the Internet Postmaster Mailbox for unsent messages. You define the Internet Postmaster Mailbox Number on the User Management > Properties for New User Web page.	For more information, see: • Adding the postmaster mailbox on page 43 • Configuring the postmaster mailbox number on page 45	As necessary or once a week.
13	Check the uninitialized mailboxes report to identify mailboxes that were never initialized. This report is useful when you migrate from older Messaging releases. You can remove unused mailboxes and free-up unused licenses.	For more information, see Viewing the uninitialized mailboxes report on page 282.	Monthly.
14	Check the dormant mailbox report to identify inactive mailboxes.	For more information, see Running the system evaluation report on page 286.	Monthly.
15	Run traffic reports. Use the traffic information to troubleshoot the system and to improve system efficiency.	For more information, see: • Viewing the Internet messaging traffic on page 286 • Running the traffic measurement report on page 289	As necessary.

Number	Tasks	Links	Frequency
16	Run audits. Audits can reconcile conflicts among databases by checking for inconsistencies and when possible, updating the information in databases to correct the Messaging problems.	For more information, see: • Messaging database audit on page 300 • Performing the voice messaging database audit on page 301 • Running Audit on page 302	As necessary.
17	Back up the data.	For more information, see: • Back up and restore overview on page 211 • Backing up system files on page 213	Nightly according to the routine automatic schedule. Perform the backup task as necessary: • After making major system changes. • After creating new users. • When experiencing system problems to avoid losing information entered since the last backup. • When a partial backup occurs to avoid losing the data sets that the system did not back up.
18	Verify that the backup completed successfully.	For more information, see Viewing backup logs on page 220.	Daily.

Number	Tasks	Links	Frequency
19	Restore the data.	For more information, see: • Back up and restore overview on page 211 • Performing a restore on page 221	Perform the restore task as necessary: • If the storage server data is lost or corrupted. • If the system fails because of data loss. • If the hard disk fails.
20	Remove unused enhanced lists.	For more information, see Administering an ELA List on page 176.	As necessary.
21	Check the software management logs. Use the log to review information about the installation, update, or removal of software packages.	For more information, see: • Storage server logs overview on page 252 • Viewing the software management logs on page 259	As necessary.

Messaging database audit

Messaging databases work independently of each other under the direction of a set of software and hardware processes. These processes coordinate the files, databases, and system hardware. Since the system handles the databases separately, one database might contain information that conflicts with another database. For example, if you delete a user from the Messaging database, other databases might still contain messages addressed to that user or mailing lists that include the name of the deleted user.

Audits can reconcile such conflicts among databases to check for inconsistencies and when possible, update the information in databases to correct the Messaging problems. For example, audits delete all references to a deleted user, which includes deleting the name of the user from the mailing lists and canceling message deliveries to that user. Audits run automatically or the administrator can run audits when required.

Performing the voice messaging database audit

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **Messaging DB Audits (Storage)**.
2. Click one of the links to perform an audit.

   The system displays the audit name and the result code, which indicate that the audit is running.
3. Wait for the audit to finish or perform one of the following steps:
   - Click **Abort** to partially stop the audit and exit the page.
   - Click **Back** to go to the Messaging DB Audits (Storage) Web page.
4. If the audit fails:
   a. Resolve any active alarms and rerun the audit.
   b. If the audit fails again, contact the remote service center.

Messaging Database Audits (Storage) field descriptions

Click	To
History	View audit history
Start Mailboxes Audit (Mailboxes, Mailbox Data)	Audit mailboxes
Start Mailing Lists Audit (Mail Lists, Delivery Data)	Audit mailing lists
Start Voice Names Audit (Voice Names)	Audit names
Start Network Data Audit (Machine Translations, Network Translations, Network Data) **Note:** This audit is available only if the system has Digital Networking.	Audit network data

Click	To
Start Subscriber Data Audit (Subscribers, Delivery Data)	Audit user data
Start Nightly Audit (Nightly, Delivery Data)	Perform nightly audit
Start Weekly Audit (Weekly, Delivery Data, Network Data, Mailbox Data)	Perform weekly audit

Audit History field descriptions

Name	Description
Date	The audit date.
Time	The time of audit.
Start/End	The status of audit: start or end.
Audit	The audit type.
Result	The status of audit.

Running Audit

The Running Audit Web page displays the current status of a audit. The system displays the audit name and result code, which indicate that the audit is running.

Click **Abort** to partially stop the audit and exit the page, or click **Back** to go to the Messaging Database Audits (Storage) Web page.

Verifying or restarting the LDAP processes

The LDAP Status/Restart (Storage) Web page displays the current status of the LDAP processes. You can manually restart the LDAPFE and LDAPCORP processes. Use LDAPFE and LDAPCORP to administer the Messaging data from the internal and external client respectively.

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **LDAP Status/Restart (Storage)**.
2. Verify if all the processes are in the **UP** state.
3. If any process is not in the **UP** state, click **Restart** to manually start the process.

Note:

To start all LDAP processes, you must restart the Messaging application.

LDAP Status/Restart (Storage) field descriptions

Field Name	Description
slapd	slapd is the core process for LDAP in Messaging. Messaging functions only when slapd is running. To restart slapd, you must bring the Messaging system to the **DOWN** state. An **UP** state indicates that slapd is running. The **DOWN** state indicates that slapd is not running, and you must restart Messaging.
Ldapfe	Ldapfe is the process to perform administration from the Web pages. An **UP** state indicates that Ldapfe is running. The **DOWN** state indicates that Ldapfe is not running. You can perform administration through the Web pages until you restart this process.
Ldapcorp	Ldapcorp is the process to perform administration from external LDAP clients. The firewall must also be open to perform administration through external clients. To check the firewall status, on the **Administration** menu, click **Server (Maintenance)** > **Security** > **Firewall**. An **UP** state indicates that Ldapcorp is running. The **DOWN** state indicates that Ldapcorp is not running. You can perform administration through the external LDAP clients until you restart this process.

Octel Aria migration

Messaging Release 6.2 supports migration of user mailbox properties, messages, recorded names, and user greetings from Octel Aria 3.10 and 3.11 systems.

The migration of Octel systems include:

- Octel 250 and 350 system
- Octel *0* type mailboxes
- Voice messages

The migration does not include:

- Personal Distribution Lists
- Auto Attendants
- Fax messages
- Hidden mailboxes
- Non-delivery notifications
- Passwords
- Multilingual capabilities of the Aria server

There must be sufficient client license seats to cover the number of mailboxes for migration. You must enable client access for all mailboxes in CoS. Migrated messages show the status in the Messaging mailbox as read or unread and priority as urgent or regular.

Importing Octel Aria data

Note:

Avaya Professional Services must import the Octel Aria data using the *craft* login.

Before you begin

- The name of the Octel Aria data file must be in the `Octel_NAG_xxxxxxx.zip` format for Names and Greetings and `Octel_MSG_xxxxxxx.zip` format for Messages. xxxxxxx can be any alphanumeric characters except _. For example, `Octel_NAG_stormy92000-92999.zip`.

  If you need to change the mailbox number to a different one, you must provide a file named `Octel_NAG_xxxxxxx.ext` or `Octel_MSG_xxxxxxx.ext`. For example, if you need

Comments? infodev@avaya.com

to change the mailbox number from 92000 to 8888892000, you must provide a mapping file with the name as `Octel_NAG_stormy92000-92999.ext`.

- Avaya Professional Services must upload the Octel Aria data file to Messaging using the Communication Manager upload files screen.
- Ensure that the Messaging system is running.
- No other import is running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **Octel Aria Migration**.
2. Select the Octel Aria data file that you want to import.
3. Click **Import**.
   The system imports the Octel Aria data.
4. You can view the logs of the import after the import is complete by selecting the appropriate log file.
5. Click **View logs**.
   The system displays the log data.

Octel Aria Migration field descriptions

Field	Description
Octel Aria zip file	The Octel Aria data zip file for import.
Log file	The logs of the import process.

Button	Description
Import	To import the Octel Aria data zip file.
View logs	To view the logs of the import.

IMAP/SMTP administration

Administering general options

Use the fields on the Internet Messaging: General Options and Settings Web page to manage the Messaging resources used for processing emails. The fields also define how Internet Messaging affects other Messaging features.

Procedure

1. On the **Administration** menu, click **Messaging** > **IMAP/SMTP Settings (Storage)** > **General Options**.
2. In the **Maximum number of INCOMING SMTP sessions** field, select the required value.
3. In the **Maximum number of OUTGOING SMTP sessions** field, select the required value.
4. Click **Save**.
   The system saves the settings.

Internet Messaging: General Options and Settings field descriptions

Name	Description
Maximum Number of INCOMING SMTP Sessions	SMTP sessions require processing resources and affect the quality of service. If the system receives several email messages simultaneously, the system starts additional sessions to accommodate the additional traffic up to the administered limit. If you increase this number, the number limits the possibility of the machine sending messages to temporarily becoming unable to send emails. Although email servers automatically retry sending messages, most email clients require users to resend the message.

Name	Description
	After setting this field and turning on Internet Messaging, select **Server Reports** > **IMAP/SMTP Traffic (Storage)** and check the volume of email traffic in the **SMTP Outgoing** area.
Maximum Number of OUTGOING SMTP Sessions	The system uses the maximum number of sessions only if needed. If a large volume of outbound email is queued for delivery, the system starts additional sessions up to the administered limit. After setting this field and turning on Internet Messaging, select **Server Reports** > **IMAP/SMTP Traffic (Storage)** and check the volume of email traffic in the **SMTP Outgoing** area.

Mail options

Use the Mail Options Web page to specify how to manage emails and to define configuration information used in processing incoming and outgoing emails.

Depending on the selections you make on this page, the outgoing email address is resolved as follows:

- If you specify a mailbox gateway, the system sends all outbound emails to the gateway for delivery to the destination.
- If you do not specify a mailbox gateway, the system uses the configured Domain Name server to look up the host.domain portion of the outgoing user@host.domain email address.
- If the DNS lookup fails, the system checks the administered host files entries for host.domain.
- If all the methods fail, the message is marked as undeliverable and returned to the sender.

Configuring the mail options

Procedure

1. On the **Administration** menu, click **Messaging** > **IMAP/SMTP Settings (Storage)** > **Mail Options**.
2. Enter the appropriate information in the fields.

3. Click **Save**.
   The system saves the settings.
4. If you configure the server alias, you must reload the user list.

   For more information, see Loading lists on page 175.

   If the system is part of a message network, you must request a remote update from the message-networking server to ensure message delivery to the messaging network.

Mail Options field descriptions

Name	Description
Mailbox Gateway Machine Name	The TCP/IP hostname of the mailbox gateway. Your communication network routes all outbound emails through the gateway you select from this drop-down list. The system populates the list using the External Hosts Web page. For example, *94221@machine.domain.com*.
Server Alias	An alternate hostname of the mail gateway. For example, *94221@domain.com*. Using aliases, organizations can create easily recognized email addresses for their clients and employees. For example, *extension@domain.com*.
Warn about undeliverable mail after	The number of days after which the system notifies users that the system did not deliver the user message. Internet Messaging attempts delivery for the specified number of days. Then, the sender receives a warning that includes a part of the message for identification purposes. Attempts to deliver the message continue even after the warning notification. The number of times the server attempts delivery depends on the number of days set in this option.
Report undeliverable mail and delete it after	The number of days after which the system returns an undeliverable message to the sender. After this threshold passes, the sender receives an email that the message was

Name	Description
	undeliverable with the original message attached. The system no longer attempts to deliver the message.
Check for mail every	The time interval for checking the message queues. The system sends and delivers outgoing and incoming messages immediately. However, if the system does not send or deliver a message immediately, the system performs a check after the specified interval and delivers all messages in the queue.

Verifying the IMAP/SMTP status

Procedure

On the **Administration** menu, click **Messaging** > **IMAP/SMTP Settings (Storage)** > **IMAP/SMTP Status**.
The system displays the IMAP/SMTP status.

IMAP/SMTP status field descriptions

The Internet Messaging: IMAP/SMTP Status Web page displays the latest snapshot of the Internet messaging operation.

Name	Description
Internet Message status	Displays whether the inbound and outbound email delivery processes are operating.
Percent of media space in use (contains queues)	Displays the percentage of used space in the media file system. The media file system contains messages and various system data, including temporary files, Internet messaging queues, and logs.
Number of incoming messages in queue	Displays the actual number of messages waiting in the incoming message queue when the system read the data. If the setting is high, the system allows more messages into the queue and uses more

Name	Description
	space. If the system uses more space, message storage or processing is affected.
Number of outgoing messages in queue	Displays the actual number of messages waiting in the outgoing message queue when the system read the data.
Number of SMTP receive/send sessions running	Displays the number of SMTP sessions currently active for processing incoming and outgoing messages.
Number of POP3 client retrieval sessions running	Displays the number of sessions currently active for servicing POP3 users, such as POP3 connections created with the Outlook email application.
Number of IMAP4 client retrieval sessions running	Displays the number of sessions currently active for servicing IMAP4 clients, such as IMAP4 accounts established with Outlook Express.

Voice Equipment Diagnostics

You can perform the following diagnostics on an installed analog-line interface card:

- Busying out voice channels on page 310.
- Diagnosing the voice equipment on page 311.
- Displaying the voice equipment status on page 313.
- Releasing the voice channels on page 314.

Busying out voice channels

Busying out voice channels takes channels out of service. The system does not forward calls out of service channels. You can busy out more than one channel.

Note:

Do not busy out all voice channels at once, as no channels remain for incoming calls.

Procedure

1. On the **Administration** menu, click **Messaging** > **Telephony Diagnostics (Application)** > **Busy**.

Comments? infodev@avaya.com

2. Enter the appropriate information in the fields.
3. Click **Busyout**.
   When the state change is complete, the system displays the Busyout of Voice Equipment Web page.

Busyout of Voice Equipment field descriptions

Caution:

If you select **yes** in the **Change immediately** field, the system disconnects all calls in progress. Do not select **yes** unless call traffic is extremely low. If you select **no**, the voice cards or channels busy out when the voice calls or channels are free. Busying out voice cards and channels when the voice cards and channels are free of calls might take a longer time, but the calls are not disconnected.

Field Name	Description
New State	Specifies the state of the equipment. This field is always set to **manoos**.
Equipment	This field is always set to **Channel**.
Equipment Number	Specifies the number of the channel. You can enter channel numbers in several forms: • A single number. For example, 1. • A range of numbers. For example, 0-2. • A list of single numbers. For example, 0,1,2. • A list of single numbers and ranges. For example, 0, 1-2.
Change immediately	Select **yes** to change the state immediately, even if the channel is busy. Select **no** to change the state when the channel becomes idle.

Diagnosing the voice equipment

Note:

The system uses SIP integration between Communication Manager and Messaging. Hence, the following steps are not applicable to Messaging.

Procedure

1. On the **Administration** menu, click **Messaging** > **Telephony Diagnostics (Application)** > **Diagnose**.
2. Enter the appropriate information in the fields.

   Note:

   Do not diagnose all analog-line interface cards or channels at the same time, as there will be no available channels to accept incoming calls.
3. Click **Diagnose**.
   Depending on the selected equipment, diagnosis can take several minutes. The system displays the Voice Board Diagnostics Web page.
4. If the system displays either of the following messages, the system did not detect a working telephone line connected to the voice port. Perform steps 5 to 7.

   ```
   No loop current on channel number
   Channel number changed to state FOOS
   ```
5. Verify that you have properly connected the telephone line to both the interface card and the telephony server.
6. Verify that the analog line is set up properly on the telephony server.
7. Verify that the telephony server port has a dial tone by removing the analog line. Plug in an analog telephone, and listen to the handset for the dial tone.
   - If there is a dial tone, the analog-line interface card is defective.
   - If there is no dial tone, the telephony server is faulty. Verify the wiring and administration of the telephony server.
   - If the system displays the following message, the system did not detect a dial tone. However, the system did detect loop current, which could be a result of excessive load on the analog-line interface card. If you see the following message, perform steps 8 and 9.

     ```
     Diag TRnumber: No dial tone frequencies set
     ```
8. Verify that the analog lines are distributed over several analog-line interface cards.
9. Verify that the telephony server administration for the ports is valid.
10. If the system displays one of the following messages, the channel or card is not working. You must replace the analog-line interface card:

    ```
    Channel number changed to state BROKEN
    Card number changed to state BROKEN
    ```
11. If the card is NONEX, nonexistent, verify that you have properly fixed the card in the slot.

If the card is not fixed properly, fix the card properly and follow the procedures for correcting power supply.

Diagnose Equipment field descriptions

Caution:

If you select **yes** in the **Immediate Diagnosis** field, the system disconnects all calls that are in progress. Do not select **yes** unless call traffic is extremely low. Diagnosing voice cards only when the voice cards are free of calls can take longer, but no calls are disconnected.

Field Name	Description
Equipment to diagnose	Displays the equipment to diagnose as **Card**.
Equipment Number	Specifies the number of the card.
Immediate Diagnosis	Immediate diagnosis takes specified channels out of service immediately even if a call is in progress. Select **no** to wait until all specified channels are idle before beginning the diagnosis.

Displaying the voice equipment status

Procedure

On the **Administration** menu, click **Messaging** > **Telephony Diagnostics (Application)** > **Display**.
The system displays the information about the voice equipment.

Display Voice Equipment field descriptions

Field Name	Description
Card	Identifies the circuit card on which the channel resides.
Port	The virtual port number.
Channel	The virtual channel number.

Field Name	Description
State	The current status of the channel, as follows: • In-service (INSERV): The normal state. • Facility-out-of-service (FOOS). • Manually-out-of-service (MANOOS). • Hardware-out-of-service (HWOOS). • broken: Diagnostics did not pass on the card. Hence, you might need to replace the card.
Time	The time and date of the last change in the state of the channel.
Service	The associated service name or a DNIS designation indication.
Phone	The telephony server extensions that correspond to the channel.
Group	—
Opts	The equipment options: • talk • TDM
Type	The type of voice card.

Releasing the voice channels

Releasing voice channels places all the channels in service. In-service channels can accept and process calls. You can also release one or more individual channels.

Procedure

1. On the **Administration** menu, click **Messaging** > **Telephony Diagnostics (Application)** > **Release**.
   After the channels are released, the state of the equipment is changed to inserv.
2. Enter the appropriate information in the fields.
3. Click **Release**.
   When the state change is complete, the system displays the Release of Voice Equipment Web page.

Release of Voice Equipment field descriptions

Field Name	Description
New State	Specifies the state of the equipment. This field is always **inserv**.
Equipment	This field is always **Channel**.
Equipment Number	Specifies the number of the channel. You can enter channel numbers in several forms: • A single number. For example, 1. • A range of numbers. For example, 0-2. • A list of single numbers. For example, 0,1,2. • A list of single numbers and ranges. For example, 0, 1-2.

Security

Generating a certificate signing request

To reduce the errors that customers receive while logging into the SMI, customers might want to install their own vendor signed certificates on their Messaging systems. These certificates are signed by a certificate authority (CA) and are built for a particular system name, that is, fully qualified domain name.

The Certificate Signing Request (CSR) Web page enables you to manage the CSRs present on the server. The customer can generate a CSR to send to their CA, that is, Entrust, VeriSign, and so on. If there are outstanding requests in `etc/opt/ecs/certs/signing-requests`, the system displays the CSR Web page. If there are no outstanding signing requests, the system displays the CSR - Form Web page. The system allows a maximum of four certificate-signing requests to be outstanding at any given point of time.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Certificate Signing Request**.

2. Complete the fields with the appropriate information. For more information, see Certificate Signing Request - Form field descriptions on page 317.

   If there are outstanding certificate service requests, click **New Request** and complete the fields.

3. Click **Generate Request**.
   The system displays the Certificate Signing Request - Display Web page. You must send the certificate output from the Certificate Signing Request - Display Web page to the CA.

4. Copy and paste a portion of the CSR data, from the *Begin Certificate Request* area to the *End Certificate Request* area, into a notepad and save the notepad.

5. Click **Continue**.

6. Send the notepad document to the CA.

   The CA vendor sends a Messaging certificate file to the customer. The certificate file includes the .pem or .crt extension. Messaging voice mail uses this certificate. If you install this certificate, the system eliminates the error seen by customers when the customers log in to the Messaging SMI.

   The certificates are chained certificates. To install a chained certificate, you must install the CA Root certificate. Some certificate authorities, such as VeriSign require you to install an Intermediate certificate. After you load the Root certificate and Intermediate certificate, if required, you can install the Messaging certificate.

   The customer must download the Root certificate and install this certificate before installing other certificates on the Messaging system. The following links are for the Root certificates of VeriSign and Entrust.

   Note:

   Larger customers might have a contract with the vendor and therefore have direct access to the Root and Intermediate certificates. The customer follows vendor directions on how to download the Root certificate. If an Intermediate certificate is required, the website of the vendor provides information on how to obtain the Intermediate certificate.

   - VeriSign: http://www.verisign.com/repository/roots/root-certificates/PCA-3G2.pem. Copy the certificate information in the `PCA-3G2.pem` file.
   - Entrust: https://www.entrust.net/downloads/root_request.cfm. Enter your name, company name, and email address and then select the **Entrust Root CA** check box and select the **Server/Host Type** as *Apache (OpenSSL)*. Click **Accept**. After you receive the email, copy the certificate information in the `PCA-3G2.pem` file.

7. After the customer has all the certificates, Root, Intermediate, and Messaging, the customer can download these certificates to the Messaging system. The customer must first copy these certificates to the `/var/home/ftp/pub` directory.

To copy these certificates to the `/var/home/ftp/pub` directory, see Downloading files on page 317.

Certificate Signing Request - Form field descriptions

Certificate Field	Field Value
Country Name (2 letter code)	Enter the name of the country where the Messaging server is located. The country name is a 2-letter code.
State or Province Name (full name)	Enter the name of the state or province where the Messaging server is located.
Locality Name (e.g. city)	Enter the name of the locality where the Messaging server is located.
Organization Name (e.g. company)	Enter the name of the organization applying for the certificate-signing request.
Organization Unit (e.g. section/ department)	Enter the name of the organization unit applying for the certificate-signing request.
Common Name (e.g. host name)	Enter the host server name or the server FQDN. If the corporate LAN has a name for this server, the Common Name field defaults to that value.
RSA Key Size (bits)	Select the default length of the RSA key.
This is a CA certificate (see help)	The system displays this field only if the server is a main server. By default, main servers obtain their certificate from Authentication File System (AFS) at http://rfa.avaya.com. LSP and ESS servers obtain their certificates by issuing a certificate-signing request to their main server. The main server must have a CA certificate to sign the request. You can install this type of certificate only in the Messaging repository.

Downloading files

Use the Download Files Web page to download files onto the Avaya server from another server across the network using HTTP protocol. Typical files to download include new license or

authentication files, IPSI firmware upgrades, system announcements, or keys.install files, all of which may be used with network timeservers.

Before you begin

To use the Download Files Web page, the server must be able to access the:

- Corporate LAN and typically, the DNS server for routing and name resolution
- Web server(s) in the selected URLs reference.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Miscellaneous** > **Download Files**.
2. To download files from your system to the Avaya server, select **File(s) to download from the machine I'm using to connect to the server** and then:
   a. Click **Choose File** or enter the path to the file that resides on your system. You can specify up to four files to download.
   b. Click **Open**.
3. To download files from a Web server to the Avaya server, select **File(s) to download from the LAN using URL** and then:
   a. Specify up to four files to download by Universal Resource Locator (URL) address.
   b. Specify the complete URL. For example, `https://networktime.com/security/keys.install`
   c. If you require a proxy server for an external Web server that is not on the corporate network, you must enter the details in the `server:port` format.
      - Enter the name of the proxy server such as network.proxy or IP address.
      - If the proxy server requires a port number, add a colon (:).
   d. Click **Download**.
   The system displays the Download Files Results Web page .

   After the system copies the certificates to the `/var/home/ftp/pub` directory, you must install the certificates using the SMI. For more information, see Adding a trusted certificate on page 319.

Download Files field descriptions

Name	Description
File(s) to download from the machine I'm using to connect to the server	Download files from your system to the server.

Comments? infodev@avaya.com

Name	Description
File(s) to download from the LAN using URL	Download files from a Web server to the Avaya server.
Proxy Server	If you require a proxy server for an external Web server that is not on the corporate network, you must enter the details in the `server:port` format.

Trusted Certificates

Use the Trusted Certificates Web page to manage the trusted certificate repositories for the server. The Trusted Certificates Web page displays all the installed certificates. Use this page to add a certificate, copy an existing certificate to other repositories, or delete a certificate from repositories.

Displaying a trusted certificate

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Trusted Certificates**.
2. Select a certificate and click **Display**.
   The Trusted Certificates - Display Web page displays the content of the selected certificate.

Adding a trusted certificate

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Trusted Certificates**.
2. On the Trusted Certificates Web page, click **Add**.
3. On the Trusted Certificates - Add Web page, in the **PEM file containing certificate** field, enter the file name of a trusted certificate.

   Note:

   A trusted certificate must be a Certificate Authority (CA) certificate.

   The certificate that you want to add must have a .pem or .crt extension and must be in the `/var/home/ftp/pub` directory on the server. If the file extension is .der,

you must change the file extension to a .pem extension. You must change the extension using the `-openssl x509 -inform der -in certificate.der -out certificate.pem` command at the command-line.

4. Click **Open** to validate the certificate.

   After successful verification, the Trusted Certificates - Add Web page displays the issued-to, issued by, and date of expiration information for the certificate you want to add.

   Note:

   If the file does not include a valid certificate, the system displays an error message instead of the certificate content.

5. Enter a file name to store the certificate by the same name in each repository.

   The system displays several repositories to which you can add the certificate. The repositories include: C=CM related such as SIP PKI; W=Web server, M = Messaging.

   If you add the Root certificate to a Messaging certificate, select W.

6. Select the check box for the appropriate repositories in which you want to install the certificate.

7. Click **Add**.

   The system verifies the following:

   - The certificate name has a .pem or .crt extension. If the file name does include a crt extension, the system deletes the entered extension and replaces the extension with a crt extension prior to creating the file.
   - The certificate name is unique.
   - The certificate is not a duplicate certificate with a new name.

   Note:

   If you fail to install a certificate in one repository, the failure does not affect the installation in other repositories.

   The system displays a success message and the Root certificate for the certificate authority in the Trusted Certificates Web screen.

   Note:

   After you install the Root certificate, if you need to install an Intermediate certificate, the website of the vendor directs you on the steps to obtain the Intermediate certificate.

   After you install the certificates, install the Messaging certificate. For more information, see Adding a server and application certificate on page 323.

Deleting a trusted certificate

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Trusted Certificates**.
2. On the Trusted Certificates Web page, select a certificate.
3. Click **Remove**.
   The Trusted Certificates – Remove Web page shows the **File**, **Issued To**, **Issued By**, **Expiration Date**, and **Trusted By** information for the selected certificate.
4. Select the appropriate check boxes to delete the certificate from one or more repositories.
5. Click **Remove**.
   The system deletes the trusted certificate.

Copying a trusted certificate

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Trusted Certificates**.
2. On the Trusted Certificates Web page, select a certificate and click **Copy**.
   The system displays the Trusted Certificates - Copy Web page that includes the selected certificate content and the list of trusted repositories.
3. In the **copy to these trusted repositories** area, select the check boxes for one or more repositories.
4. Click **Copy**.
   The Web page verifies the following:
   - If the file name is unique and does not already exist
   - If a certificate is duplicated with a new file name

   Note:

   If you fail to install a certificate in one repository, the failure does not affect the installation in other repositories.

Trusted Certificates field descriptions

Name	Description
File	The name of the individual certificate file. The file name is the same in all the repositories.
Issued To	The name of the company to whom the certificate is issued.
Issued By	The name of the company that issued the certificate.
Expiration Date	The expiry date of the certificate.
Trusted By	The list of single letter identifiers for the repositories in which you install the certificate. • **A**. Authentication, Authorization, and Accounting Services. For example, LDAP. • **C**. Communication Manager • **W**. Web Server • **M**. Messaging

Server/Application Certificates

Use the Server/Application Certificates Web page to manage the server and application certificate repositories for the server. The Server/Application Certificates Web page displays all the installed certificates. Use this page to install a certificate, copy an existing certificate to other repositories, or delete a certificate from repositories.

Displaying a certificate

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Server/ Application Certificates**.
   The system displays the Server/Application Certificates Web page.
2. Select a certificate entry.
3. To display the content of the certificate chain, click **Display**.

The Server/Application Certificates - Display Web page displays the content of the certificate chain.

Adding a server and application certificate

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Server/ Application Certificates**.
   The system displays the Server/Application Certificates Web page.
2. Click **Add**.
   The Messaging certificate file must be present in the `/var/home/ftp/pub` directory and the file must have a .pem or .crt extension.
   The system displays the Server/Application Certificates - Add Web page.
3. Enter the file name of the Messaging certificate.
   The certificate must be a PKCS#12 file or a file in the pem format.
4. Enter the password of the certificate that you want to add.
5. Click **Open** to validate the certificate.
   The system verifies the following:
   - The certificate has a .pem or .crt extension. If the certificate has a different extension, the system deletes the extension and replaces the extension with a .crt extension.
   - The certificate name is unique.
   - The certificate is not a duplicate certificate with a new name.

   After successful verification, the Server/Application Certificates Web page displays the issued-to, issued by, and date of expiration information for each of the added certificates in the chain.

   If the file does not contain a valid certificate, the system displays an error message instead of the certificate content.
6. Select the appropriate repositories check box in which you want to install the certificate.

   Note:

   The system does not prompt you to enter a file name to store the certificate. By default, the file name is `server.crt`.

   In the case of a single server and application certificate chain, the server sub-directory of a repository is limited to a single file for a single certificate chain and

the file is `server.crt`. This certificate represents an identity and only one identity is supported. The system overwrites the existing `server.crt` file.

7. Click **Add**.
   After successful installation of the server certificate, the SSL client, for example browser of client machine accessing the SMI, the system prompts you regarding the change. After you accept the change, the system displays the previously accessed page.

   Note:

   If you fail to install a certificate in one repository, the failure does not affect the installation in other repositories.

Deleting a certificate

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Server/ Application Certificates**.
   The system displays the Server/Application Certificates Web page.
2. Select a certificate entry.
3. To delete the certificate chain, click **Remove**.
   The Server/Application Certificates – Remove Web page displays the file name, issued-to, issued by, date of expiration, and installed-in information for the first certificate in the selected certificate chain.
4. Select the appropriate check box to delete the certificate from a single repository or from an arbitrary combination of repositories if the certificate is installed in more than one repository.
5. Click **Remove**.
   The system deletes the certificate.

Copying a certificate

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Server/ Application Certificates**.
   The system displays the Server/Application Certificates Web page.

2. Select a certificate entry.
3. Click **Copy**.
   The Server/Application Certificates - Copy Web page displays the certificate content of the first certificate in the chain along with a list of all other repositories from which you can select any combination.
4. Select the appropriate repositories check box in which you want to install the selected certificate.
5. To install the selected certificate in the selected repositories, click **Copy**.

   For each repository where you installed the certificate, the system overwrites or creates the server.crt and server.key files.

Note:

If you fail to install a certificate in one repository, the failure does not affect the installation in other repositories.

Server/Application Certificates field descriptions

Name	Description
File	The name of the certificate file, which is the same in all repositories. The system stores the server certificates in a concatenated file as a certificate chain.
Issued To	The name of the company to whom the certificate is issued.
Issued By	The name of the company who issued the certificate.
Expiration Date	The date of the certificate expiration.
Installed In	The list of single letter identifiers for the repository in which you installed the certificate.

Authentication File

The Authentication File Web page provides information about the Avaya authentication file currently installed on the system. You must install the authentication file using the System Platform console domain.

This file contains the logons and passwords that Avaya services personnel use to access the Avaya server. If you have a maintenance contract, the Avaya services personnel update this file regularly.

Note:

The system blocks access to the Messaging software if a valid authentication file is not present on every Avaya server.

The authentication file is created on an Avaya services support system and downloaded to the Avaya server. You can change the file only using this support system. To change authentication information, you must replace the entire file.

If the authentication file is missing or corrupted, the system denies access to the Avaya server. However, this does not prevent the Avaya call-processing software from running, but the system blocks further administration until a new authentication file is installed using the System Platform console domain.

To access the authentication file, on the **Administration** menu, click **Server (Maintenance)** > **Security** > **Authentication File**.

Authentication File field descriptions

Name	Description
AFID	The authentication file ID.
Product	The product name of the authentication file. For Messaging, the product name is SP System Platform.
Release	The major product release of the authentication file.
Common Name	The host name of the Messaging server.
Authentication file generation date	The date when the system generated the authentication file.
Authentication file generation time	The time when the system generated the authentication file.
Authentication file request type	The request type of the authentication file. The types of requests are New System/ Existing System, Same Release/Existing System, and Upgrade.
ASG key type	The type of Avaya Security Gateway. The types of ASG keys include new and existing.

Name	Description
Password type	The type of password.
AFS Request ID	The request ID of AFS.

Firewall

Use the Firewall Web page to view the current rules for the IPv4 and IPv6 firewall.

On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Firewall**.

Install Root Certificate using Internet Explorer

About this task

Use the Install Root Certificate Web page to install an Avaya root certificate on your computer to establish Avaya as a trusted CA.

Caution:

The system does not support Netscape Navigator. You must use Internet Explorer.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Install Root Certificate**.
2. Click **Install**.
3. In the **File Download** dialog box, click **Open**.

   Important:

   Do not save this file to disk.
4. In the **Certificate** dialog box, in **General** tab, click **Install Certificate**.
   The Certificate Manager Import Wizard guides you through the process. Accept all the default values and wait for the install to complete.
5. Click **Finish**.
   A Root Certificate store message may appear.
6. Click **Yes** to add the certificate to the Trusted Root Certification Authorities store.
7. Click **OK** a couple of times to close the open dialog boxes.

SSH Keys

Secure Shell is a security program to log in to another computer over a network, to run commands from a remote machine, and to move files from one machine to another. The program features include authentication and secure communications over insecure channels. Secure Shell is a replacement for rlogin, rsh, rcp, and rdist.

If you are using ssh slogin instead of rlogin, the system encrypts the entire logon session including transmission of password. Hence, the system does not allow an outsider to collect passwords.

The system displays the fingerprint on the Web page while connecting to the server through the SSH. Before you accept and connect to the server, compare fingerprints with the one that the system displays on the **SSH Keys** Web page.

To access the SSH Keys Web page, on the **Administration** menu, click **Server (Maintenance)** > **Security** > **SSH Keys** .

SSH Keys field descriptions

Name	Description
Current SSH public keys	The system displays the installed keys.
Generate new SSH keys	Select one of the following keys: • **RSA keys for SSHv2** • **DSA keys for SSHv2** For more information about SSH, visit: http://www.ssh.org.

Enabling or disabling services on the server

Use the Server Access Web page to enable or disable various services on the Avaya server. If enabled, use the selected service to allow the communications application running on another computer or server to access the server.

To use a service, you must enable the service and the firewall for that particular service.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Server Access**.

2. To enable or disable the following services on the Avaya server, click the **Enable** or **Disable** option:
   - FTP Server (21)
   - Telnet Server (23)
   - SAT (Telnet 5023)
   - SSH Server (SCP/SFTP 22)
   - High Priority SSH (2222)
   - SAT (SSH 5022)
3. Click **Submit**.
   The system saves the changes.

Role-Based Access Control

With Role-Based Access Control (RBAC), you can control privileges on the application server and storage server based on the roles you define for the business. Using roles, you can fine-tune the security and administration of the Messaging system. A role defines a group of users who have certain privileges. You can create roles to allow or restrict access to the SMI Web pages.

You can group the access rights by a role name. Profiles for access to SMI Web pages are named access masks. Using the access mask, you can restrict the access permissions. Messaging provides some default access masks and names, such as System Profile, Customer Super User Profile, and Customer Non-Super User Profile. You can use the SMI Web pages to create a new Web access mask profile and enable access as desired.

Adding a Web Access Mask

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Web Access Mask**.
2. On the Web Access Mask Web page, click **Add**.
3. On the Add Access Mask Web page, enter a new mask number in the **Enter new Access Mask Number** field.
4. Select one of the following options:
   a. **Create by copying values from Access Mask number**. Also, enter a value in the text box.
   b. **Create and set all values to enable access**
   c. **Create and set all values to disable access**

5. Click **Submit**.
   The system saves the changes.

Changing a Web Access Mask

About this task

Use the Change Access Mask Web page to change access mask names and permissions to menu items. Menu items with check marks are accessible to that access mask.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Web Access Mask**.
2. On the Web Access Mask Web page, in the **User-Defined Access Masks and Names** area, select the check box next to an access mask.
3. Click **Change**.
4. On the Change Access Masks Web page, enter the name of the mask in the text box next to the access mask number.
5. In the **Editable** column, select or clear the check boxes to set permissions.
6. Click **Submit**.
   The system saves the changes.

Deleting a Web Access Mask

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Web Access Mask**.
2. On the Web Access Mask Web page, in the **User-Defined Access Masks and Names** area, select the check box adjacent to an access mask.
3. Click **Delete**.
4. On the Delete Access Mask Web page, verify the access mask is the one you want to delete, and then click **Submit**.
   The system deletes the access mask.

Web Access Mask field descriptions

Purpose

Use the Web Access Mask Web page to restrict individual logins in the SUSERS and USERS login groups based on membership in a secondary Linux login group.

Access mask base displays the current profile base number.

Note:

Changes to the profile base also affect your access to Communication Manager.

Access masks and names

There are two types of access masks:

- Default. Default masks are 0-17, 18, and 19. You cannot edit these masks.
- User defined. You can change the user-defined access masks.

The default access masks are:

Mask	Name
0-17	System Profiles
18	Customer Super User Profile
19	Customer Non-Super User Profile

You can add, change, delete, or view the user-defined access masks. Each mask applies to a specific secondary Linux login group.

Working with Web Access Masks

Use the following buttons to change masks:

Button	Description
Add	To add a new mask.
Change	To change the existing access masks.
Delete	To delete an existing mask.
View	To view properties of the selected access masks.
View All	To view properties of all the user-defined access masks.
Select All	To select all user-defined access masks listed on the page.
De-select All	To de-select all user-defined access masks listed on the page.

Button	Description
File Sync	To update the LSP and ESS servers on a duplicated system after you add, change, or delete profiles.

View access mask and view all access masks

The View Selected Access Masks and View All Access Masks Web pages displays the Web menu items accessible for the selected or all access masks. The system lists the menu items by category in the left navigation pane. Menu items with check marks are accessible for that particular access mask.

Using diagnostic tools

Testing the alarm origination

Use the Test Alarm Origination Web page to verify that the system logs the alarms properly and sends the alarms to the administered location. After you run the test, the system raises an alarm.

If the alarming system uses a modem and you have logged in remotely, log off as soon as possible after running the test.

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **Alarm Origination**.
   The system displays the Test Alarm Origination Web page.
2. To activate the test alarm, click **Run Test**.
   The test alarm becomes active and stays active for 30 minutes after which the alarm retires automatically.

Next steps

To view alarm logs, click **Display Alarm Log**. For more information, see Viewing the alarm logs on page 256.

Testing the LDAP connection

Use the Test LDAP Connection Web page to verify that you have administered the networked machines correctly. The test connects to the LDAP server on the selected machine using the administered IP address, port, name, and password.

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **LDAP Test Connection**.
2. Select a machine from the drop-down list.
3. Click **Run Test**.
   The system displays the test results.

Testing the SMTP connection

Use the SMTP connection test to check low-level network connectivity. Local or remote service technicians can perform fault isolation of network problems during the installation and the testing of Internet Messaging..

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **SMTP Connection**.
   The system displays the Internet Messaging: SMTP Connection Test Web page.
2. To check if the host email system is working, enter the **IP Address or Host Name** of the destination machine.
3. Click **Run Test**.
   The system displays the test results.

Internet Messaging: SMTP Connection Test field descriptions

Name	Description
IP Address or Host Name	The IP address or fully qualified internet host name of the destination machine to check if the host email system is working.

Testing the POP3 connection

Use this test to verify low-level network connectivity. Local or remote service technicians can perform fault isolation of network problems during the installation and the testing of Internet Messaging.

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **POP3 Connection**.
   The system displays the Internet Messaging: POP3 Connection Test Web page.
2. To check if the host email system is working, enter the **IP Address or Host Name** of the destination machine.
3. Click **Run Test**.
   The system displays the test results.

Internet Messaging: POP3 Connection Test field descriptions

Name	Description
IP Address or Host Name	The IP address or fully qualified internet host name of the destination machine to check if the host email system is working.

Testing the IMAP4 connection

Use this test to check low-level network connectivity. Local or remote service technicians can perform fault isolation of network problems during the installation and the testing of Internet Messaging.

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **IMAP4 Connection**.
   The system displays the Internet Messaging: IMAP4 Connection Test Web page.
2. To check if the host email system is working, enter the **IP Address or Host Name** of the destination machine.
3. Click **Run Test**.

The system displays the test results.

Internet Messaging: IMAP4 Connection Test field descriptions

Name	Description
IP Address or Host Name	The IP address or fully qualified internet host name of the destination machine to check if the host email system is working.

Testing the mail delivery

Use this test to check high-level email connections. Local or remote service technicians can perform fault isolation of network problems during the installation and the testing of Internet Messaging.

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **Mail Delivery**.
   The system displays the Internet Messaging: Mail Delivery Test Web page.
2. In the **Sender** field, enter the mailbox extension or the email handle of the sender.
3. In the **Sender's Password** field, enter the email password of the sender.
4. In the **Recipient** field, enter the email address of the recipient.
5. Click **Run Test**.
   The system displays the test results.

Internet Messaging: Mail Delivery Test field descriptions

Name	Description
Sender	The mailbox extension or the email handle of the sender.
Sender's Password	The email password of the sender.
Recipient	The email address of the recipient.

Testing the name server lookup

Use the Name Server Lookup test to determine whether you can look up a system using the domain name servers assigned on the Network Configuration Web page. If the system can look up domains, the system can also deliver messages to these domains.

Run the Name Server Lookup test for the Messaging server and the mail gateway.

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **Name Server Lookup**.
   The system displays the Test Name Server Lookup Web page.
2. Enter the Internet host name or IP address of the system for which you want to run the test.
3. In the **Select DNS Server** field, select a DNS server.
4. In the **Record Type** field, select the type of information that you want to retrieve.
5. Click **Run Test**.
   The system displays the test results.

Test Name Server Lookup field descriptions

Name	Description
Enter internet host name or IP address	The Internet host name or IP address of the system for which you want to run the test.
Select DNS Server	Select a DNS server from the drop-down list.
Record Type	The type of information you want to retrieve.

Name Server Lookup Results field descriptions

Name	Description
***Record Type* Record Lookup**	The results of the name server lookup. Use the test to determine whether you can look up a system through the domain name

Name	Description
	servers assigned on the Network Configuration Web page. If the system can look up the domains, the system can also deliver messages to these domains.

Running application server diagnostics

Use the Diagnostics (Application) Web page to run one or more diagnostics tests to evaluate the various components of the application server. For some tests, you need to specify additional parameters before running the test. All test results display the local time of the client machine from where you run the diagnostics test.

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **Diagnostics (Application)**.
2. In the **Select the test(s) to run** field, select a test or all tests.
   Depending on the test that you select, the system displays the additional fields.
3. Enter the appropriate field values for the associated test that you want to run.
4. Click **Run Tests**.
   The system displays the test results or errors in the **Results** area.
5. If you want to download and save the results, click **Download Results**.

Next steps

You can download the diagnostics logs of all the diagnostics that you run on the application server. To download the logs, go to **Messaging** > **Logs** > **Diagnostics Results (Application)**. For more information, see Accessing diagnostics results on page 274.

Diagnostics (Application) field descriptions

Diagnostic Test	Description
All tests	Runs all available tests. You must enter at least one MWI extension to run the MWI diagnostic test.
Application Distributed Cache	Tests that the distributed cache server is up and running. Additionally, checks that data can be read, written, and deleted.

Diagnostic Test	Description
Call-out	Calls out to a specified extension. When you pick up the phone, you should hear a test greeting. The parameters to be specified are: • **Telephone number**. The telephone number that the application server calls. • **Port number**. (Optional) The port or line that the application server uses to make the call.
Cluster	Tests the connectivity and the cluster configuration of the application server. The test connects to all ADCSs in a cluster to see if the ADCSs respond.
Communication	Tests the communication facilities of the application server, including the TTS port, the voice browser, the Web server, the Messaging application, and the line states. For serial (SMDI/MCI) integrations only, the system also tests the SMDI or MCI link.
MWI	Tests the Message Waiting Indicator (MWI) configuration. The system turns the MWI light for the extension on and off during the test. You must specify the following parameters: • **Extension number**. The extension number of the user. • **MWI port number**. (Optional) The port number.
Messages to Deliver	Queries the ADCS through TUI to check the number of messages that the system needs to deliver to the storage server or the user mailbox.
User and Contact Lists	Queries the local cache on the application server for a user or contact. You should specify the following parameters: • **Type of user/contact list**. The contact list that is queried to locate the specified user or contact. You can select either **User List** or **Global Address List**. • **Mailbox number or email address**. The mailbox number or email address of the user or contact to be located.

Diagnostic Test	Description
Voice Messaging Application	Diagnoses the state of the Messaging application and the communication link to the AxC.

Ping

Use the Ping Web page to obtain information about your network. Use the ping command to:

- Test whether a specified address in your network is working.
- Obtain information about how quickly and efficiently your network is processing data packets.
- Use the diagnostic information to manage your network.

Using the ping command

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Diagnostics** > **Ping**.
2. On the Ping Web page, enter the appropriate information in the fields.
3. To run the ping command, click **Execute Ping**.
   If the ping is successful, the Ping Result Web page displays a brief summary that displays the number of packets sent and received.

   The summary also displays the minimum number, the maximum number, and the average of the round-trip times.

Ping field descriptions

Name	Description
Host Name Or IP address	Select this option and enter the host name or IP address that you want to ping. If you enter a value in the **Host Name or IP Address** field, you must select **IPv4** or **IPv6**, or both. If you select both **IPv4** and **IPv6** and run the **`ping`** command, the Ping

Name	Description
	Results Web page displays the ping results for both the networks.
IPv4	Select this check box if the system has IPv4 connectivity. By default, the system selects this check box.
IPv6	Select this check box if the system has IPv6 connectivity. The system displays this option only if the system has IPv6 connectivity. **Important:** The IPv6 Address field is limited to a specific customer set and not for general use.
Do not look up symbolic names for host addresses	Select this check box to ping the server by using an IP address. If you do not select this check box, the system looks up symbolic names for the host addresses. The system uses the domain name server that translates the IP address to a symbolic name. The ping command fails if the domain name server is unavailable.
Bypass normal routing tables and send directly to a host	Select this check box to ping a local host on an attached network. You must select this check box to bypass the routing table and ping a local host through an interface that has no route. If the host is not on a network, the ping is unsuccessful. The system displays an error message.
Use alternate interface ____ as the source	The system displays this field only if you selected **IPv6** in the **Host Name Or IP Address** area. Select an alternate Ethernet interface as the source from the list. The system uses the selected interface to run the **`ping`** command.

Ping results

When you run the ping command, the system displays the Ping Results Web page to display whether the command was successful. The following sections describe successful and unsuccessful ping results:

Successful ping results

If the **ping** command runs successfully, the Ping Results Web page displays a brief summary similar to the following:

```
PING www.asite.com (135.9.4.93) from 135.9.77.30 : 56 (84) bytes of data.
64 bytes from www.asite.com (135.9.4.93): icmp_seq=0 ttl=245 time=6.3 ms
64 bytes from www.asite.com (135.9.4.93): icmp_seq-1 ttl=245 time=6.3 ms
--- www.asite.com ping statistics ---
2 packets transmitted, 2 packets received, 0% loss
round-trip min/avg/max = 0.3/3.3/6.3 ms
```

Unsuccessful ping results

If the **ping** command does not run successfully, the Ping Results Web page displays an error message. Each error message indicates one or more possible problems, such as:

`100% packet loss`. This error message can indicate a variety of things, including:

- `The network host is down.`
- `The host is denying the packets.`
- `The network is down.`
- `The ping was sent to the wrong address.`

`Packets are rejected`. This message indicates that the host is rejecting the packets.

`Packets did not reach the host`. This message indicates a problem with the network. Therefore, the ping packets cannot reach the host.

Traceroute

Use the Traceroute Web page to view the full connection path between your site and another network address. The **traceroute** command tracks how IP packets move through the gateways that connect the Avaya server network hardware. To trace the IP packet route, the **traceroute** command launches short-lived probe packets in the connection path and then listens for a time exceeded reply from a gateway.

Use the **traceroute** command to evaluate the hops taken between the links in your TCP/IP network. Hops are short, individual trips that packets take from one router to another on the route to their destinations.

Using the traceroute command

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Diagnostics** > **Traceroute**.
2. On the Traceroute Web page, enter the appropriate information in the fields.

3. To view the connection path, click **Execute Traceroute**.
   The system displays the results.

Traceroute field descriptions

Name	Description
Host Name or IP address	You must select **IPv4** or **IPv6**, or both. If you select both **IPv4** and **IPv6** and run the **traceroute** command, the Traceroute Results Web page displays the traceroute results for both the networks.
IPv4	Select this check box if the system has IPv4 connectivity. The system selects this option by default. If you select **IPv4**, the system displays the **Use alternate IPv4 address ____ as the source address** field in the **Options** area on the Traceroute Web page.
IPv6	Select this check box if the system has IPv6 connectivity. The system displays this option only if the system has IPv6 connectivity. If you select **IPv6**, the system displays the **Use alternate interface ____ as the source** field in the **Options** area on the Traceroute Web page. **Important:** The IPv6 Address field is limited to a specific customer set and not for general use.
Print address numerically	Select this check box to print the hop addresses numerically rather than by symbolic name and number. If you do not select this check box, the system looks up symbolic names for the host addresses. To do so, the system uses the domain name server, which translates the IP address to a symbolic name. If the domain name server is unavailable, the **traceroute** command is unsuccessful.

Name	Description
Bypass routing tables and send directly to a host	Select this check box to run the **traceroute** command to a local host through an interface that has no route. You must select this check box to run the **traceroute** command to a local host on an attached network. If the host is not on a network that is directly attached, the **traceroute** command is unsuccessful, and the system displays an error message.
Use alternate IPv4 address ____ as the source address	The system displays this field only if you select **IPv4** in the **Host Name or IP Address** field. Select an alternate IPv4 address as the source address from the list.
Use alternate interface ____ as the source	The system displays this field only if you select **IPv6** in the **Host Name Or IP Address** field. Select an alternate Ethernet interface as the source from the list. The system uses the selected interface to run the **traceroute** command.

Traceroute results

When you run the **traceroute** command, the Traceroute Results Web page displays if the command is successful. The following sections describe successful and unsuccessful traceroute results.

Successful traceroute results

If the traceroute command runs successfully, the Traceroute Results Web page displays a summary similar to the following:

```
traceroute to server.mycompany.com (192.168.1.126), 30 hops max, 38 byte packets

1 server1.mycompany.com (192.168.1.254) 0.324 ms 0.226 ms 0.206 ms

2 server2.mycompany.com (192.168.2.254) 0.446 ms 0.372 ms 0.288 ms

3 server.mycompany.com (192.168.1.126) 0.321 ms 0.227 ms 0.212 ms
```

As shown in the example, the traceroute output in the first line differs from the output in the subsequent lines. The following sections describe the traceroute output:

First line of output

The first line of traceroute output describes the parameters within which the command was run.

The output displays:

- Destination host name and IP address: *server.mycompany.com* (192.168.1.126)
- Maximum number of hops: 30 hops max
- Packet size: 38 byte packets

Subsequent lines of output

The subsequent lines of traceroute output describe each hop completed for the traceroute. These lines display:

- Hop number: 1, 2, and 3
- Address of the gateway computer, which is the host name, followed by the IP address. For example, *server.mycompany.com* (192.168.1.254).

  If you select to print the addresses numerically, the system displays no host name in the output. For example:

  1 192.168.1.254 0.778 ms 0.590 ms 0.216 ms

  2 192.168.2.254 0.507 ms 0.449 ms 0.311 ms
- Round-trip time to the gateway computer. For example, 0.324 ms 0.226 ms 0.206 ms.

Note:

Each hop is measured three times. If you see an asterisk (*) in the round-trip time part of the output, the * indicates that a hop has exceeded the limit.

Unsuccessful traceroute results

If the traceroute command does not run successfully, the Traceroute Results Web page displays information about the error as follows:

```
traceroute: unknown host www.unknown.com. This is because the host
www.unknown.com cannot be reached.
```

Netstat

Use the Netstat Web page to obtain information about server connections running over TCP/IP. The **Netstat** command provides statistics about network-related data structures such as domain sockets routing tables and Internet connections.

Running the Netstat command

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Diagnostics** > **Netstat**.

2. On the Netstat Web page, enter the appropriate information in the fields.
3. To obtain information about server conditions, click **Execute Netstat**. The system displays the results in the Netstat Results Web page.

Netstat command field descriptions

Field	Description
Output type	
View the status of network connections by listing the open sockets [default]	To view the active Internet connections, except those associated with the server processes.
View all sockets	To view the state of all domain sockets, including those used by server processes.
View listening sockets only	To view only those active domain sockets that are used by server processes.
Display routing table	To view the routing table for specific IP addresses.
Display networking interfaces	To view the kernel interface table, which provides information about the packet traffic on the network interfaces.
Output format	
Show numeric addresses	To ensure that the addresses display numerically on the Netstat Results Web page, select **Show numeric addresses**. If you do not select this option, the system searches for symbolic names for the addresses using the domain name server. If the domain name server is unavailable, the **NetStat** command is unsuccessful.
Show only the following address families	
inet	To view the IPv4 routing table entries. This option limits the statistics or address control block reports to the INET addresses. The socket type is AF_INET.
inet6	To view the IPv6 routing table entries.
unix	To limit the statistics or address control block reports to UNIX addresses.

Field	Description
	The socket type is AF_UNIX, that is, the local machine socket. To view results for inet, inet6, and UNIX address families on the same page, select all the options.

Netstat results

Purpose

The system displays the information on the Netstat Results Web page depending on the output type you select when using the **Netstat** command. The following sample results combine output for inet and UNIX address families and are not applicable to each output type selection.

The following sections describe the two types of output.

inet address families

Active Internet connections (w/o servers)						
Proto	**Recv-Q**	**Send-Q**	**Local Address**	**Foreign Address**	**State**	**PID/ Program name**
tcp	0	0	mycom-srv1:www	Srv2.:2402	Established	831/
tcp	0	0	mycom-srv1:telnet	Srv3:1077	Established	1969/

Name	Description
Proto	The protocol used by the socket.
Recv-Q	The number of bytes not copied by the user program connected to the socket.
Send-Q	The number of bytes not acknowledged by the remote host.
Local Address	The host name of the socket.
Foreign Address	The remote host name and port number of the socket.
State	The state of the socket. The state might have one of the following values.
ESTABLISHED	The socket has established a connection.

Comments? infodev@avaya.com

Name	Description
SYN_SENT	The socket is actively attempting to establish a connection.
SYN_RECV	The socket has received a connection request from the network.
FIN_WAIT1	The socket is closed, and the connection is shutting down.
FIN_WAIT2	The connection is closed, and the socket is waiting for a shutdown from the remote end.
TIME_WAIT	The socket is waiting after being closed to handle packets still in the network.
CLOSED	The socket is not being used.
CLOSE_WAIT	The remote end has shut down, and the remote end is waiting for the socket to close.
LAST_ACK	The remote end has shut down, and the socket is closed. The socket is waiting for acknowledgment.
LISTEN	The socket is listening for incoming connections.
CLOSING	Both local and remote sockets are shut down, but all the data is still not sent.
UNKNOWN	The state of the socket is unknown.

UNIX address families

Active UNIX domain sockets (w/o servers)						
Proto	**RefCnt**	**Flags**	**Type**	**State**	**I-Node**	**Path**
unix	7	[ ]	DGRAM		33148	/dev/log
unix	0	[ ]	DGRAM		42350	
unix	0	[ ]	DGRAM		38530	

Name	Description
Proto	The protocol used by the socket.
RefCnt	The reference count of processes attached through this socket.

Name	Description
Flags	Is used for unconnected sockets if their corresponding processes are waiting for a connect request.
Type	The type of socket access: SOCK_DGRAM, SOCK_STREAM, SOCK_RAW, SOCK_RDM, SOCK_SEQPACKET, SOCK_PACKET RAW.
SOCK_DGRAM	The socket is used in Datagram mode without connections.
SOCK_STREAM	The socket is a stream socket.
SOCK_RAW	The socket is used as a raw socket.
SOCK_RDM	The socket is for reliably delivered messages.
SOCK_SEQPACKET	The socket is a sequential packet socket.
SOCK_PACKET RAW	The socket is an interface access socket.
UNKNOWN	The socket is unknown.
State	The state of the socket. For a list of possible socket states, see the description for inet address families.
I-Node	The associated file for this socket, shown as an I-node number.
Path	The path name of the processes attached to the socket.

Server information

Verifying the status of the application role

About this task

The System Status (Application) Web page displays the status of the various processes used for the application role and the connection status with the AxC. The system displays the status of the following items on this page:

- Application software release
- System uptime

- AxC IP address
- Time
- Voice Messaging Application
  - Last known AxC status
- Voice Browser
  - Text-To-Speech
- User Data Migration
- Application Distributed Cache Server
- Storage Synchronizer

Note:

After you upgrade Messaging to release 6.2, you must ensure that the **User Data Migration** process is in *Not Running* state before restarting the Messaging system.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Information** > **System Status (Application)**.
   The system displays the results.
2. To view the updated results, click **Refresh**.

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 on the Voice Channels (Application) Web page.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Information** > **Voice Channels (Application)**.
2. In the **Refresh Rate** field, enter the new interval.
   The interval can be between 1 to 30 seconds.
3. Click **Display**.

Note:

If you reduce the refresh rate, the system needs more resources that could adversely the affect system performance. Monitor your system after changing the interval to ensure that the system performance is unaffected.

Voice Channels (Application) field descriptions

Name	Description
Refresh Rate	The new refresh rate interval. The default setting for the refresh rate is 5 seconds. The interval can be between 1 and 30 seconds.

Voice Channel Monitor field descriptions

Name	Description
Channel	The channel number.
Calls Today	The calls on that channel today.
Voice Service	The voice service.
Service Status	The service status.
Caller Input	The caller input.
Dialed Digits	The dialed digits.

Viewing the cache statistics

Cache server statistics display how the system handles cache in a cluster or single application server if there is no cluster. The system tracks cache server statistics by cluster hit rates and storage usage.

If the system retrieves information from the message store, the system saves the data in the application server cache. If an application server needs the data again, the system queries the cache first, resulting in less requests going back to the message store.

In a clustered environment, if the data is not present on the application server, the application server queries other application servers for the data before requesting the data from the message store.

Procedure

On the **Administration** menu, click **Messaging** > **Server Information** > **Cache Statistics (Application)**.
The system displays the cache server statistics.

Monitor cache statistics

The system tracks cache server statistics by cluster hit rates and storage usage. Hits represent the data required for the transaction that the system finds in the cache. The system tracks this data in terms of local counts and cluster-wide counts of voice mail messages.

- Local cache is the cache on the application server that you are viewing.
- Cluster cache refers to the collective cache of the cluster, that is, all application servers in the cluster. In a single application server, local and cluster cache are the same.

  Cluster statistics include statistics based on inbound cache requests from other application servers in the same cluster. Cluster statistics are the same on all application servers in the cluster.

In terms of storage usage, the system tracks the cache in terms of local and cluster cache. The system uses the storage quota to support the cache statistics. Use the **Clear counters** button in the Counters panel to clear the cache statistics values.

The following table provides descriptions to the key components of the Cluster Hit Rates panel.

Key	Description
Local Cache Hits (this appliance)	The percentage of times the system made a request and found the required data in the local cache.
Cluster Cache Hits (peer appliances)	The percentage of times the system made a request and found the required data in another application server cache in the cluster.
Email Backend Hits (email servers)	The percentage of times the system made a request and found the required data in the email servers.
Total read attempts	The total number of times the system attempted to read a cache. The attempt might fail if there is a value in the **Failed writes** field.
Failed writes	The total number of times the system attempted to read a cache but failed.

Advanced application server settings

Reload application server cache

Use the Reload Caches panel to force cache reloads, as required. During normal operations, you do not need to perform manual reloads of the data caches of the application server. However, reloading system caches ensures that the system synchronizes the data displayed in the administration interface of the application server with the Avaya X Connector (AXC) server.

You might need to use the forced operation in following situations:

- Force a manual reload of **User List**, **Global Address List**, **System Greeting**, or **Classes of service** if there are network problems that have impaired communications between the AXC and the application server. For example, cache reloads are required if you have made changes to extensions associated with local users or caller applications subsequent to initial creation.

  After adding users, you must reload the GAL or wait for the system nightly maintenance to view the users on the Remote Users reports page.

  Note:

  Reloading the GAL is dependent on the size of the list and the responsiveness of the AXC and message store servers. Other cache reloads vary in time, depending on the size.

- Force a reload of the System Greeting audio file if the audio file has been updated on the AXC server.
- Force a reload of the Classes of Service definition file if this file has been updated on the AXC server.
- Force a synchronization of the Distributed Cache whenever the application server has been offline for a long period. The application server synchronizes the data with the AXC server to which the application server is bound.

System Operations field descriptions

Name	Description
Reload Caches	

Comments? infodev@avaya.com

Name	Description
User List	To reload the user list, click **Reload**.
Global Address List	To reload the global address list, click **Reload**.
System Greeting	To reload the system greeting, click **Reload**.
Classes Of Service	To reload the CoS, click **Reload**.
Application Distributed Cache (ADCS)	To synchronize ADCS, click **Synchronize**.
System Operations Advanced	
Restart Voice Messaging Application	To restart the voice messaging application, click **Restart**.
Restart Voice Browser	To restart the voice browser, click **Restart**.
Restart Text-To-Speech engine	To restart the Text-To-Speech engine, click **Restart**.
Restart ADCS	To restart ADCS, click **Restart**.
Local Directory Cache	
Clear the local directory cache (excludes ADCS)	To clear the local directory cache, click **Clear**.
Distributed Cache (ADCS) Maintenance	
General	
Delete ADCS cache directory and restart ADCS and Voice Messaging Application	To delete the ADCS cache directory and restart ADCS and Voice Messaging Application, click **Delete Cache**. The system deletes the system configuration and user information from the cache. Additionally, the system deletes undelivered broadcast messages and voice mail messages. The system drops all active calls immediately, and the Messaging system is temporary unavailable.
Clear all data in ADCS cache on this application server	To clear all data in the ADCS cache on this application server, click **Clear Cache**. The **Results** area displays the number of objects cleared from the cache.
Clear all recorded greetings and names in ADCS cache on this application server	To remove any recorded greeting or name inconsistencies in the cache between the application and storage servers, click **Clear Greetings/Names**.

Name	Description
	Additionally, the system removes recently recorded greetings and names that are not relayed to the message store. The **Results** area displays the number of objects cleared from the cache.
User-Specific	
Clear a user's data in ADCS cache on this application server	
User's email address	The email address of the user.
Types of objects to delete	The type of objects to delete. The options are: • **Voicemail objects** • **Non-voicemail objects**

Configuring the timeouts information

Procedure

1. On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **Timeouts**.
2. Enter the appropriate information in the fields.
3. Click **Apply**.

   Some of the changes require the system to restart processes. This results in the following:

   - The system immediately drops all active VoIP calls.
   - The network connection between the message store and the application server is temporarily lost.
   - Application Distributed Cache System is unavailable, possibly for several minutes.
   - The system does not record new messages during this time.
   - New settings are not reflected when the system is running in offline mode.

Timeouts field descriptions

Field	Description
Communication with AxC	
Web Services communication timeout	The Web services communication time-out period in milliseconds.
Caller Application communication timeout	The Caller Application communication time-out period in milliseconds.
Short synchronous connection timeout	The short synchronous connection time-out period in milliseconds.
Short synchronous socket timeout	The short synchronous socket time-out period in milliseconds.
Variable synchronous connection timeout	The variable synchronous connection time-out period in milliseconds.
Variable synchronous socket timeout	The variable synchronous socket time-out period in milliseconds.
Variable asynchronous connection timeout	The variable asynchronous connection time-out period in milliseconds.
Variable asynchronous socket timeout	The variable asynchronous socket time-out period in milliseconds.
Long asynchronous connection timeout	The long asynchronous connection time-out period in milliseconds.
Long asynchronous socket timeout	The long asynchronous socket time-out period in milliseconds.
Exchange Synchronizer retry period	The Exchange synchronizer retry period in minutes.
Exchange Synchronizer retry attempts	The retry attempts for the Exchange synchronizer.
Exchange Synchronizer connection timeout	The Exchange synchronizer connection time-out in milliseconds.
Personal Contact List Refreshing Interval	The personal contact list refreshing interval in minutes.
Contact lists fetch timeout	The contact lists fetch time-out in milliseconds.
Miscellaneous communications	
ADCS communication timeout	The ADCS communication time-out in milliseconds.

Field	Description
URLConnection connection timeout	The URL connection time-out in milliseconds.
URLConnection socket timeout	The URL connection socket time-out in milliseconds.
Offline Detection Frequencies and Timeouts	
Offline-detection polling during normal conditions	The offline-detection polling during normal conditions in milliseconds.
Online-detection polling during offline conditions	The online-detection polling during offline conditions in milliseconds.
Network ping timeout	The network ping time-out in seconds.
Offline-detection timeout for legacy subsystem	The offline-detection time-out for legacy subsystem in milliseconds.
Offline-detection timeout for web services subsystem	The offline-detection time-out for Web services subsystem in milliseconds.

Viewing the AxC address

Procedure

On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **AxC Address**.
The AxC Address Web page displays the IP address of the server where the AxC resides.

AxC Address field descriptions

Name	Description
AxC Address	
AxC IP address	The IP address of the storage server.
AxC Web Services Security	
For web services communication with the AxC, use	To use a secure connection for Web services communication with the AxC, click **https://**.

Configuring the miscellaneous information

Procedure

1. On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **Miscellaneous**.
2. Enter the appropriate information in the fields.
3. Click **Apply**.

   Some of the changes require the system to restart processes. This results in the following:

   - The system immediately drops all active VoIP calls.
   - The network connection between the message store and the application server is temporarily lost.
   - Application Distributed Cache System is unavailable, possibly for several minutes.
   - The system does not record new messages during this time.
   - New settings are not reflected when the system is running in offline mode.

Miscellaneous field descriptions

Name	Description
Appliance-to-Appliance	
Appliance-to-Appliance	The communication between the application servers. The default value is enabled.
System Parameters	
Recording format	The codec for storing messages. Options are: • **GSM**: The GSM audio encoding format has a coding rate of approximately 13 kilobits per second (kbps) or 1.6 Kilobytes per second (KBps). A message that is 1 minute long requires approximately 95.2 KB of storage space when encoded using the GSM 6.10 format. One hour of GSM 6.10 requires 5.6 MB of storage space. GSM

Name	Description
	6.10-encoded messages occupy approximately 20% of the storage space used by G.711. • **G.711**: The G.711 audio encoding format has a coding rate of approximately 64 kbps or 8 KBps. A message that is 1 minute long requires approximately 468.8 KB of storage space when encoded using the G.711 format. One hour of G.711 requires 27.5 MB of storage space. G.711- encoded messages occupy approximately five times as much storage space as GSM 6.10.
Maximum recorded name length	The maximum recorded name length.
Delete cached voice messages from the cache after	The system deletes the cache messages from the cache after the specified hours.
Advanced Cache Configuration	
Show dirty cache	The system displays the dirty cache.

Enabling core file generation

Use the Core Files Web page to specify core file generation details for the Messaging system. Depending on the settings on this page, the system creates core files when the Messaging program ends unexpectedly due to a bug.

Use the core files to find out what went wrong. The core file contains a detailed description of the program state when the system ends the core file generation.

Procedure

1. On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **Core Files**.
2. To enable core file generation, select **enabled**.
3. Enter a value in the **Max Core File Size** field.
4. Enter a value in the **Max Cores Per Application** field.
5. Click **Apply**.
   The system saves the settings.

Core Files field descriptions

Name	Description
Core Files	
Core File Generation	The options are: • To enable core file generation, select **enabled**. • To disable core file generation, select **disabled**.
Max Core File Size	The maximum value for core files size.
Max Cores Per Application	The maximum number of cores per application.

Server configurations

Configuring the network settings

Use the Network Configuration Web page to configure or view the settings for the host name, DNS domain name, DNS search list, DNS IP addresses, server ID, and default gateway.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
2. Click **Continue** at the warning.
3. Enter the appropriate information in the fields.
   For more information, see Network Configuration field descriptions on page 360.
4. Click **Change**.
   The system saves the changes.

Network Configuration field descriptions

Name	Description
Host Name	The Messaging system host name. The host name must be unique.
DNS Domain	The DNS domain name of the server. For example, company.com.
Search Domain List	The DNS search list. If there is more than one entry, use a comma (,) to separate each entry.
Primary DNS	The Primary DNS IP address.
Secondary DNS	The Secondary DNS IP address.
Tertiary DNS	The Tertiary DNS IP address.
Server ID	The unique server ID (SVID) of the server.
Default Gateway IPV4	The default gateway address of IP version 4. If the server supports IPv6 network, in the IPv6 area, enter or view the default gateway address of IP version 6.
IP Configuration	The IPv4 address and mask that are part of the IP configuration.
Mask	The number for the mask. If you are assigning an IPv4 address, you must set this field to the subnet mask that is required for this network setup. The system supports short version and long version of the mask. If you are using the short version, enter a numeric number from 1 to 32.
Functional Assignment	The indication on how to use the interface.

Static routes

Note:

Use the Static Route Web page only if instructed by the network administrator.

Use the Static Route Web page to configure a specific network route for the server to send information over the network.

Configure a static route for Messaging other than the static route for the service port. For the service port, Messaging accepts the static route only from the Console Domain (CDOM).

Each row on the Static Route Web page represents a different static network route.

Adding a static route

About this task

Use this procedure to add a static route to System Platform. Use static routes to route packets through a VPN to the Avaya Partner who is providing remote service.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Static Routes**.
2. On the Static Route Web page, select the required interface.
3. Enter the network address.
4. Enter the network mask address.
5. Enter the gateway address.
6. Click **Change**.
   The system saves the settings.

Deleting a network route

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Static Routes**.
2. To delete an existing network route, delete all the information from the fields for that route and click **Change**.
   The system saves the settings.

Static Route field descriptions

Name	Description
IP Address	The IP address of the endpoint to which the server is connecting.
Mask/Prefix	The subnet mask or prefix required for the endpoint. The range of the prefix number is 1 through 32 for IPv4 and 1 through 128 for IPv6.
Gateway	If the gateway is part of the static network route, specify the IP address for the gateway.
Interface	The Ethernet interface that is applicable for the static network route.

Viewing the display configurations

About this task

The Display Configuration Web page displays the configuration information of the Avaya server. Use the Display Configuration Web page to obtain detailed information about the hardware capabilities of the server.

Procedure

On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Display Configuration**.
The system displays the Display Configuration Web page.

Display Configuration field descriptions

Name	Description
Product	The name of the server obtained from the Basic input/output system (BIOS) information.
Physical RAM	The size of the RAM of the server.

Name	Description
Number of CPU cores	The number of physical cores or processors in the Avaya Server. For each CPU core, the system displays the CPU model and the actual clock speed. The SMP kernel is required for multiple core CPUs. Else, the system displays only one core. The maximum number of CPU cores is 8.
Disk devices	The type, interface, size, model, and serial number information of the hard disk drive on the server. The disk drives, HDD or SSD or both, are connected to the server by using the (S)ATA or the SCSI interface.
CD/DVD devices	The interface, vendor, and model information of the master or slave of the secondary controller.
SAMP type	The type and the serial number of the Server Availability Management Card.
Number of power supply	The availability of a built-in duplicated Avaya-supplied UPS.

Server maintenance

Changing the IP address and hostname of the Messaging server

Perform the steps in this topic only if you want to change the Messaging server IP address, hostname, or both.

Procedure

1. On the System Domain Network Configuration screen, change the hostname and IP address.
2. (Optional) On the following Messaging SMI Web pages, change the server IP address, hostname, or both:
   - Telephony Integration
   - AxC Address
   - External Hosts

- Trusted Servers
- Networked Servers
- Mail Options
- Miscellaneous

3. (Optional) On the Schedule Backup Web page, change the IP address.
4. Change the IP address on the telephony server, Session Manager, and any other servers.
5. Use the Networked Servers Web page to change the IP addresses on remote Messaging servers.
6. Reboot the servers on which you have changed the IP address or hostname.
7. On the Topology Web page of Messaging SMI, add the new IP address of the application server and remove the previous IP address.
8. On the System Operations Web page, click **Reload** to reload the user list.
9. Test the features related to the Web pages on which you performed the changes.

Manage updates

Use the Manage Updates Web page to manage updates. The types of updates include service pack, security service pack, kernel, and SIP Enablement Services updates. The page displays:

- The current release that is running on the server
- Mode of the server
- Updates available for the server and the corresponding status

To access the Manage Updates Web page, on the **Administration** menu, click **Server (Maintenance)** > **Server Upgrades** > **Manage Updates**.

Manage Updates field descriptions

Name	Description
Update ID	The unique update identifier. For example, the Update ID might look like the following for a kernel update: `KERNEL-2.6.18-53.AB04XYZ`.
Status	The status of the current update. The options are:

Comments? infodev@avaya.com

Name	Description
	• **Activated**: The update is functioning correctly. • **Packed**: A new update is available. • **Unpacked**: A new update is successfully unpacked. • **Pending_Commit**: The kernel update is activated, but the activation is not committed. • **Pending_Deactivate**: The kernel update is deactivated, but the deactivation is not committed.
Type	Either hot or cold, where cold means the update affects the service, hot means the update does not affect the service. The page prompts the user to continue if the update is of type cold.
View	The information about the update file.
Unpack	Unpacks the update file. The update file is read from the update repository (`/var/home/ftp/pub`).
Activate	The system activates the update file.
Deactivate	The system deactivates the update file.
Remove	The system deletes all the files associated with an inactive update. If the update is in an *unpacked* state and exists in the update repository, the system displays the *update* as *packed* after the *unpacked* version is deleted.
Commit	The system completes the current kernel update process and displays the state. The **Commit** button is unavailable if the kernel update is not in the pending state.

Viewing the status summary

The Summary Status Web page displays the status information of the Avaya servers.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Status Summary**.
2. To refresh the page periodically, click **Refresh page every __ seconds**.
3. Select the number of seconds to wait before a page refresh, or accept the default value.

   Note:

   You must click **Refresh page every __ seconds** before you click **Refresh**. Else, the system displays an error message.
4. Click **Refresh**.
   The Web page refreshes with the updated status information.

Status Summary - Refresh Mode field descriptions

Name	Description
Cluster ID	In an ESS environment, the system refers to the Module Identification Number (MID) found in the license as the Cluster ID. This number identifies a unique cluster. Each server in a duplex pair has the same Cluster ID. The MID/CLID is set by the RFA license file and you cannot the number.
ID	The ID number of the server. In an ESS environment, the system displays the ID numbers for both the active and the standby servers.
Mode	The server mode. The system displays one of the following field values: • **Not ready**: The system displays this mode during the initialization of the server or when the server is not functional. • **Standby**: This mode indicates that the server is in service, but is not active.

Name	Description
	• **Busy Out**: This mode indicates that the server is out of service. • **Active**: This mode indicates that the server is running Avaya Call Processing, that is, telephony application software.
Major Alarms	This field indicates whether there are any outstanding major server alarms. The system displays one of the following values: • **yes** • **no**
Minor Alarms	This field indicates whether there are any outstanding minor server alarms. The system displays one of the following values: • **yes** • **no**
Control Network	This field displays **X**/**Y**/**Z** values where: • **X** is the number of IPSI-connected port networks currently controlled by the server. • **Y** is the number of IPSI-connected port networks connected to the server. ESS servers establish a connection to each IPSI that the server can communicate with to advertise their priority values. • **Z** is the maximum number of administered IPSI-connected port networks. If any value cannot be determined, the system displays "??". For example, ESS servers will display ?? for the Z value until the server receives translations from the main server. If both the servers do not show the same value, the system generates a _PE alarm.
Server Hardware	The state of the hardware.

Name	Description
	The system displays one of the following field values: • **Okay**: The system found no hardware failures. • **Degraded**: The system found hardware failures. • **Blank**: The system is yet to determine any hardware failures.
Processes	The state of the server processes. The system displays one of the following values: • **Okay**: None of the processes watched by the watchdog process is incapable of being restarted. • **Communication Manager_reload**. The telephony application process has failed. • **srv_fail**: A non-ACP platform process has failed. • **crit_os**: A critical operating system service has failed. • **Blank**: The watchdog process is not running.

Viewing the process status

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Process Status**.
   The system displays the Process Status Web page.
2. In the **Content** area, click **Summary** or **Detailed**.
   For information on the fields, see Process Status field descriptions on page 369.
3. In the **Frequency** area, click **Display once** or **Refresh page every __ seconds**.
   For information on the fields, see Process Status field descriptions on page 369.
4. To display the process status of all server applications, click **View**.
   The system displays the Process Status Results Web page.

Process Status field descriptions

Name	Description
Content	
Summary	The default option provides information about each server application, including a count of the running application processes compared to the total number of processes available, such as 2/16. This field also displays the status of the server application such as up, partially up, or down.
Detailed	The option provides the same information as the summary display, but also provides information about each of the processes associated with each server application.
Frequency	
Display once	The default option displays the status results in the Process Status Results Web page. The page is not refreshed automatically even when the status changes. The setting applies to both the **Summary** and the **Detailed** areas.
Refresh page every __ seconds	The option displays the status results every few seconds, based on the value you select from the drop-down list. The setting applies to both the **Summary** and the **Detailed** areas. The range is 5 to 60 seconds.

Process Status Results field descriptions

Purpose

The Process Status Results Web page displays the status information for server applications based on the selections you make in Viewing the process status on page 368.

Application status information

Regardless of the view you chose, the system displays status information for the following applications:

Application Name	Description
Watchdog	Recovers from failures and restarts the system.
TraceLogger	Creates and maintains the log files where most Avaya Call Processing (telephony application) applications write messages.
LicenseServer	Provides security for enabling the different software features, including the ability to run the telephony application.
SME (Server Maintenance Engine)	Tests server components periodically. The SME tests components because of both specific requests and asynchronous errors.
MasterAgent	Is a gateway SNMP agent for the server. The Master Agent receives all SNMP requests, both reads and writes, to the server. The Master Agent also validates that a requester can access the requested objects, and the Master Agent calls on a specific subagent to process the request.
MIB2agent	Handles SNMP requests for objects defined in the MIB-2.
MVSubagent	Provides SNMP access to MV configuration fault and performance data.
INADSAlarmAgent	Sends alarms to the Initialization and Administration System (INADS).
GMM (Global Maintenance Manager)	Collects, processes, and reports system-wide alarms.
SNMPManager	Acts as the SNMP trap receiver for the server. The received traps are decoded and written to the syslog.
Messaging	Controls the communications sessions and features.

Process status summary format

The system default for displaying process status information is a summary display. The following is an example of a summary display:

Watchdog	16/16	UP
TraceLogger	3	Partially Up
ENV	0/1	DOWN

In this example, you can see the following information:

- The name of the application is Watchdog.
- The number of running processes compared to the total number of processes associated with the application is 16/16.
- The application status is UP. The application status is either up, partially up, down, or off.

Process status detailed format

The detailed display provides information about each server application. However, detailed display also displays information about each process associated with an application. The following is an example of a detailed display.:

```
Messaging 58/85 PARTIALLY UP
```

isg–	xad–	ac_schd–	homre–	add–
msg_sv–	adm_mgr–	fac_st–	meas_m–	acode_m–
bdm–	lip–	prc_mgr [3/3]	pcd [3/0]	border [1/3]
dm–	bs [3/3]	stn_sv–	smdr_m–	mcp–
mis_ap–	gip–	pma–	msap–	mdm–
dap–	awu–	net_st–	pam–	aap–
ps_mapm+	fg_mapd+	ps_mapn+	ps_mapa+	fg_mape+
border[3/3]	prc_mgr[3/3]	aap[3/3]	audit[10/1]	bs[3/3
gip[3/3]	pcd[3/3]	add+	msg_sv+	adm_mgr+
ps_mapa+	fac_st+	meas_m+	acode_m+	tmr_mgr+
ps_mapb+	bdm+	nt_con+	lip+	capro+
dm+	stn_sv+	smdr_m+	mcp+	mis_ap+
tcm+	mdm+	bg_mapb+	phantom+	bg_mapc+
tape_m+	com+	dap+	awu+	initmap+
net_st+	tim+	pam+	fg_mapa+	net_mgr+
isg+	hmm+	dp_mgr+	xad+	ac_schd+
bg_mapa+	fastmap+	pit+	pma+	msap+

In this example, you can see the following information:

- The name of the application is Messaging.
- The number of running processes compared to the total number of processes associated with the application is 58/85.
- The application status is PARTIALLY UP. The application status is either up, partially up, or down.
- The list of processes associated with the application. The process list shows the truncated process name, followed by a plus (+) or a minus (-) sign. For example, ps_mapm+ and isg-. The plus sign (+) indicates that the process is running and the minus sign (-) indicates that the process is not running.
- For some processes, a set of brackets [], which follows the process name, contains the number of running copies compared to the number expected. For example, prc_mgr [3/3].

Server shutdown

Purpose

Use the Shutdown Server Web page to shut down the server immediately. You can also configure the server to restart after the shutdown process.

Caution:

You must shut down the server only after business hours. If you shut down the server, the Web server stops all processes that are running. You cannot gain access to the SMI pages until the server restarts.

If you select the **Immediate Shutdown** option, the server ignores the condition of any duplicate server. The selection also affects the method in which the duplicate server takes over from the main server.

Delayed shutdown

If you select the **Delayed Shutdown** option, the system notifies all processes that the server will shut down. Before the server shuts down, the system waits for all processes to close files and perform other clean-up activities.

Immediate shutdown

If you select the **Immediate Shutdown** option, the system does not wait for all processes that are running to end before the system shuts down the server. Immediate shutdown results in data loss.

Restart server after shutdown

To restart the server after the shutdown process, select the **Restart server after shutdown** check box.

When you shut down the server, the system displays a message depending on the conditions under which you performed the action.

If you opt for a delayed shut down of the server, the system displays the following message when the system successfully begins the shut down process: `shutdownproc accepted.Global shutdown is now in progress.`

No message

If you select the option to shut down the server immediately, the system displays a blank results page, as connectivity is lost because of the server shutdown.

Shutting down the server

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Shutdown Server**.
2. On the Shutdown Server Web page, select from the following options:
   - **Delayed Shutdown**
   - **Immediate Shutdown**
3. (Optional) Select the **Restart server after shutdown** check box.
4. Click **Shutdown**.
   The system displays the confirmation screen.
5. Click **Ok** to continue.

Shutting down the application server as an emergency plan

About this task

Note:

Do not perform the following steps if your only purpose is to reroute traffic to other application servers when you restart a specific application server.

Procedure

1. On the storage server, remove the specific application server from the topology.
   For more information, see Topology field descriptions on page 102.
   Once you remove the application server, the system automatically updates the provisioning information.

   Caution:

   If you remove the specific application server from the cluster configuration, sync cache exceptions do not occur.
2. Remove the specific application server from the cluster configuration. You must perform this step on all application servers.
   For more information, see Changing the configuration of a cluster on page 130.

If you use the application server that you removed in the previous steps to send MWI requests, then the Messaging system selects a different application server based on the updated provisioning information.

Note:

Avaya has not verified manual editing of the provisioning information and hence you must not perform the same.

Viewing the software version

About this task

Use the Software Version Web page to view the software version that the Avaya server is running. Check your software version before, during, or after you install the new software.

Procedure

On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Software Version**.
The system displays the Software Version Web page.

Software Version field descriptions

Name	Description
Operating system	The release and issue number of the Linux operating system that is running the server. For example, 2.2.17-14.1s11 is the release, by field: major release, minor release, development release - sub-release, Avaya release. • i686 is the processor type. • system manufacturer which is often unknown. • **Built**: The month, day, time and year that the software release was produced. • **Contains**: The issue and load number of the software that is running on the server. • **Reports as**: The fuller version of the software release name. For example,

Name	Description
	R011x.00.1.056.0 indicates: Release string such as R011, identifies the software product release 11, and boot Image such as x, identifies the target, x is for Linux.
Major release	Such as 00. The major release number is incremented to mark a significant phase of R011 product evolution. When this happens, the minor release number is reset to 0.
Minor release	Such as 1, indicates changes within a major release. The major release and minor release numbers together are used to identify the issue of software, for example, issue 11.1.
Load number	Such as 056, is incremented for each new software build.
Final number	Additional release number. For internal use only.
Translation Saved	The month, day, and time that the software translations were last saved to the translations directory. This can change to month-day-year format depending on the elapsed time since the translations were saved. The system shows two dates because the system always saves two copies of the translations.
License installed	The month, day, and time that the license for this software release was installed. The time may be shown in the month-day-year format depending on when the license was installed.
Status	The status of the software update.
Type	The type of software version.
Update description	The template details.

Monitoring performance

Performance monitoring includes checks for traffic measurements, memory usage, and process status.

Procedure

1. To request traffic measurements from the Messaging server using the SMI, perform the following:
   a. On the **Administration** menu, click **Messaging** > **Server Reports** > **Measurements (Storage)**.
   b. On the Messaging Measurements Web page, select the required information.
   c. Click **Get Report**.
   The system displays the traffic details in a report.
2. To check memory-related details on the Messaging server using the SSH terminal, perform the following:
   a. Log in to the Messaging server using the SSH Terminal.
   b. On the shell prompt, type **`vmstat`** and click `Enter`.
   The system displays the following fields related to memory usage:
      - **`swpd`**: The amount of virtual memory used.
      - **`free`**: The amount of idle memory.
      - **`buff`**: The amount of buffer memory used.
      - **`cache`**: The amount of cache memory used.

   Check the memory usage details for the Messaging server. The values are in KiloBytes (KB).

   If the system is running, the free memory is usually low. Free memory is wasted memory, that is, memory not used for anything. Linux systems use the memory as much as possible. However, if memory is available, buffers and caches use the memory.

   In a system that functions properly, free memory can be under *50,000*, buffer and cache memory together can easily be *1,00,000* or higher, the higher the better and virtual memory must be below *2,00,000*, or ideally below *50,000*.
3. To view the status of each application or the individual processes using the SMI, perform the following:
   a. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Process Status**.
   b. In the **Content** area, click **Summary** or **Detailed**.
   c. In the **Frequency** area, click **Display once** or **Refresh Page every _ seconds**.
   d. To display the process status of all server applications, click **View**.
   The system displays the Process Status Results Web page.

Restart software

Stopping Messaging

Use the Stop Messaging Software Web page to stop the Messaging software.

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **Stop Messaging**. The system displays the Stop Messaging Software Web page.
2. To initiate a shutdown, click **Stop**.
   The system delays the shutdown process until all calls are completed. However, after three minutes the system ends all calls that remain active.

   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.
3. Click **OK**.

Starting Messaging

Use the Start Messaging Software Web page to start the Messaging software.

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **Start Messaging**. The system displays the Start Messaging Software Web 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.
2. Click **OK**.

Messaging failover behavior

In the Messaging system, the following failovers might occur:

- Application server failure: Users experience intermittent failure as there is an attempt to synchronize the cache data specifically voice messages, and that times out and causes the delay as one of the application server is not working. Administrative actions like Password Update, User Greeting Update will also fail as the data synchronization between application servers fails. Calls to the server that is not working experience fast busy.
- Storage server failure: The system goes into offline mode. In offline mode, the system does not allow administrative updates.
- Storage and application server failures: The system does not allow administrative actions and the Messaging system only allows you to leave voice messages.

Failover experience

Storage server	Application server	Experience
Up	Up	Normal Messaging scenario
Up	Down	• Users experience failure • System does not support mailbox initialization • Administration actions like password updates result in inconsistencies • Calls to the application server that is down experience fast busy
Down	Up	• Inconsistent list of voice messages • System does not support administration actions like password updates • System in offline mode • Users can leave voice messages

Storage server	Application server	Experience
Down	Down	• Complete list of voice messages is unavailable • System does not support administration actions like password updates • Calls to the application server that is down experience fast busy • System in offline mode • Users can leave voice messages

Chapter 19: Redundant Message Store

Mutare Message Mirror

The Messaging administrator can set up a backup Avaya message store that provides business continuity if the primary storage server fails. Message Mirror software continuously synchronizes the data between these storage servers.

Message Mirror runs on a separate customer-provided Windows server, which can be a virtual server. Message Mirror uses the IMAP4 and LDAP ports to connect to the Avaya message store server. You can also use the Secure IMAP4 and LDAP ports to connect to the Avaya message store server. For more information on Message Mirror, see http://www.mutare.com.

Message Mirror continuously monitors the primary Avaya message store server and copies or mirrors messages, names, greetings, passwords, and mailbox and CoS changes to a backup Avaya message store server. Message Mirror thus supports uninterrupted voice messaging in the event of an outage. Failover to the backup server is a manual process.

The message store data is synchronized between a pair of primary and backup message store servers. Optionally, you can choose to have duplicated application servers, or duplicated clusters of application servers, in two different locations to allow recovery from a complete site that is completely destroyed.

Message store redundancy with duplicated application servers

In this configuration, you can choose to have duplicated application servers, or duplicated clusters of application servers, in two different locations to allow recovery from a site that is completely destroyed.

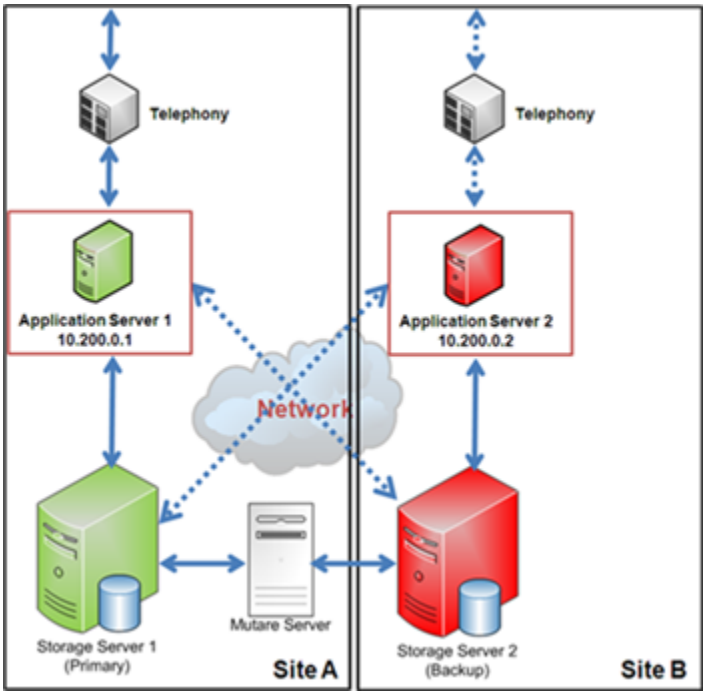
The following are examples of message store redundancy configuration with duplicated application servers.

In the following diagrams:

- Solid blue arrow represents the active status of server.
- Dotted blue arrow represents the inactive or shared status of server.

Front-end/Back-end single site configuration

In this configuration, the primary storage server and the backup storage server reside at two different sites. The application server is also duplicated at the backup site.



The following are examples of the topology page configuration.

Example

Initial setup of a new mirrored Messaging system.



Failover service to the backup Messaging system.



Failback service to the primary Messaging system.

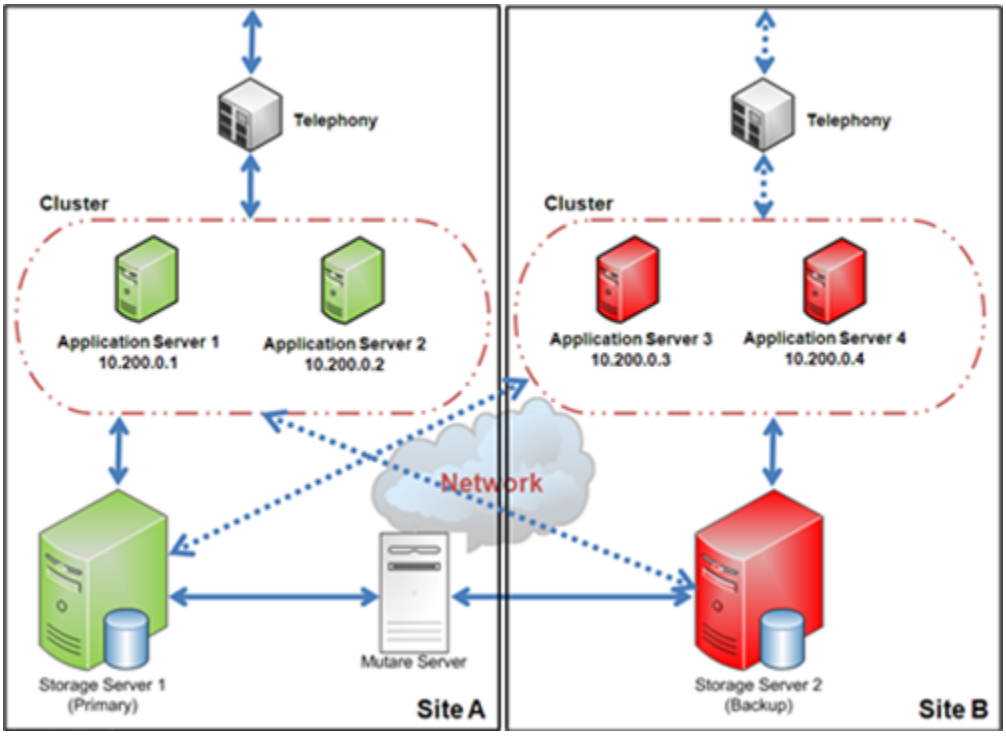


Topology configuration: Primary Storage Server

Topology configuration: Backup Storage Server

Front-end/Back-end cluster single site configuration

In this configuration, the primary storage server and the backup storage server resides at two different sites. The application server cluster is also duplicated at the backup site.



The following are examples of the topology page configuration.

Example

Initial setup of a new mirrored Messaging system.



Failover service to the backup Messaging system.



(If primary storage server is accessible)

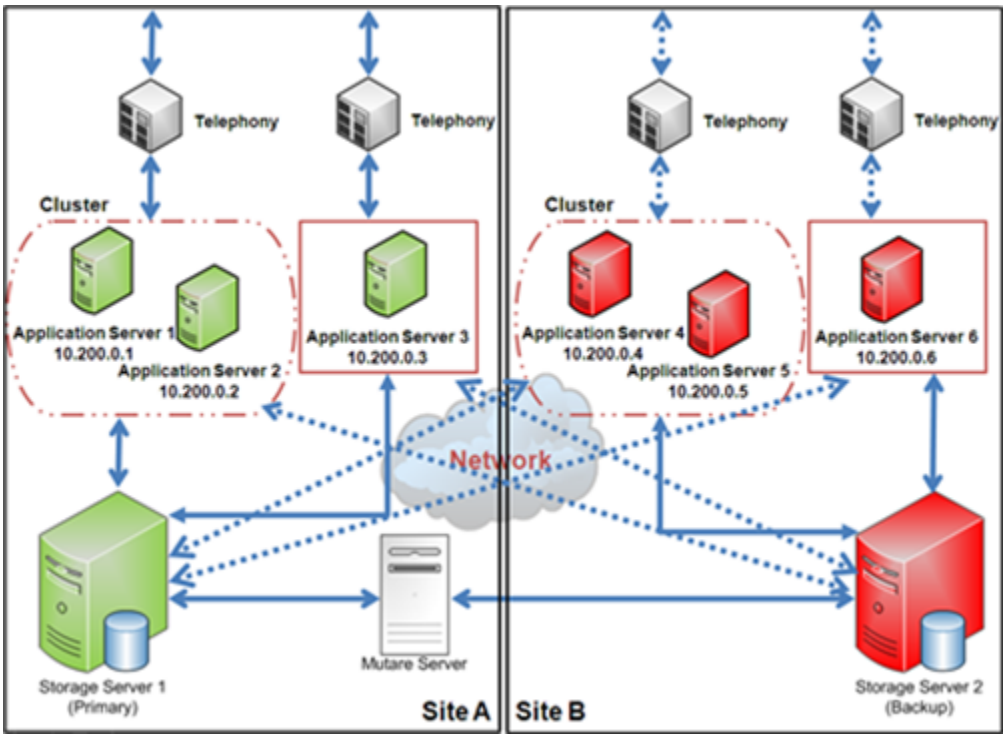
Failback service to the primary Messaging system.



Topology configuration: Primary Storage Server **Topology configuration: Backup Storage Server**

Distributed multisite configuration

In this configuration, the primary storage server and the backup storage server resides at two different sites. You can distribute application servers at different locations. The application server is also duplicated at the primary site and the backup site.



The following are examples of the topology page configuration.

Example

Initial setup of a new mirrored Messaging system.



Failover service to the backup Messaging system.



Failback service to the primary Messaging system.



Message store redundancy with shared application servers

In this configuration, application server(s) of the primary system are shared by the backup system.

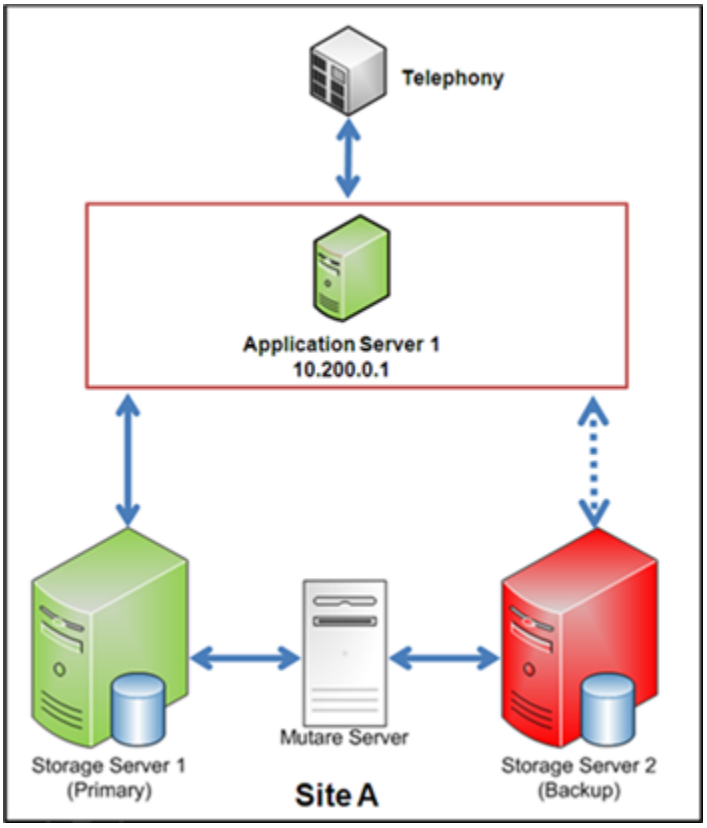
The following are examples of message store redundancy configuration with shared application servers.

In the following diagrams:

- Solid blue arrow represents the active status of server.
- Dotted blue arrow represents the inactive or shared status of server.

Front-end/Back-end single site configuration

In this configuration, the primary storage server and the backup storage server resides at a single site. The application server is shared by both the storage servers.



The following are examples of the topology page configuration.

Example

Initial setup of a new mirrored Messaging system.



Failover service to the backup Messaging system.



Failback service to the primary Messaging system.

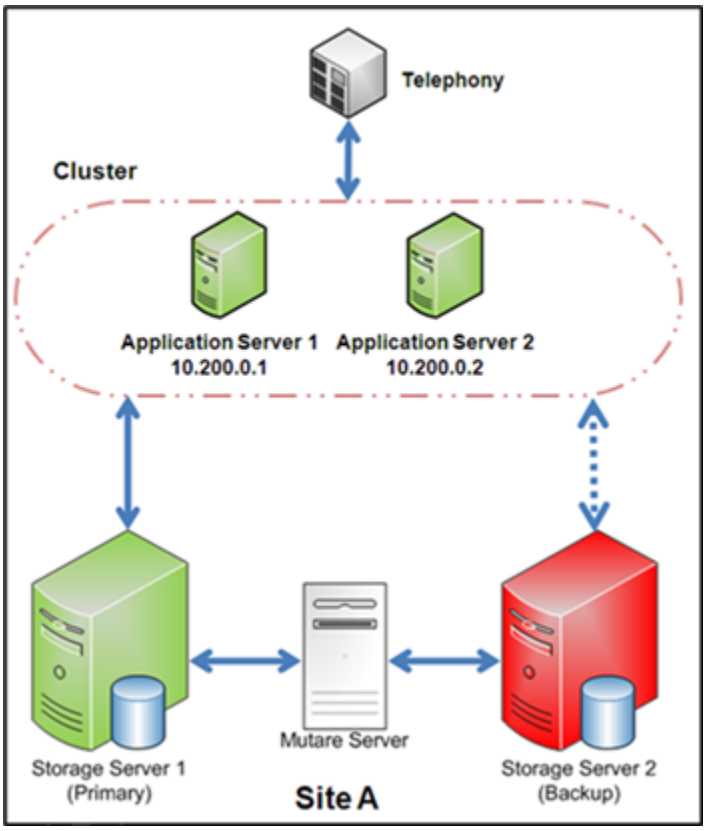


Topology configuration: Primary Storage Server

Topology configuration: Backup Storage Server

Front-end/Back-end cluster single site configuration

In this configuration, the primary storage server and the backup storage server resides at a single site. You can combine up to four application servers to form a cluster, which is shared by both the storage servers.



The following are examples of the topology page configuration.

Example

Initial setup of a new mirrored Messaging system.



Failover service to the backup Messaging system.



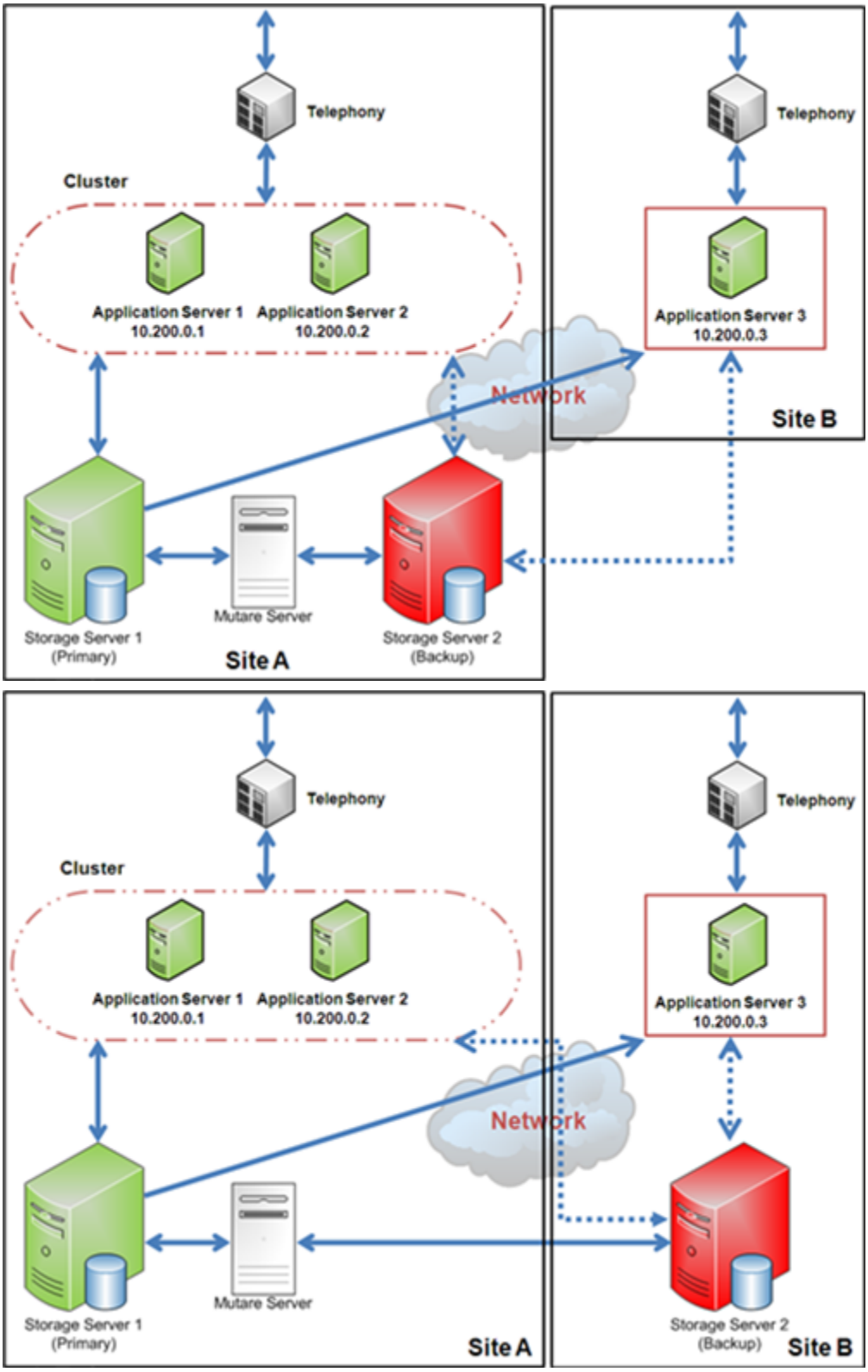
(If primary storage server is accessible)

Failback service to the primary Messaging system.



Distributed multisite configuration

In this configuration, the primary storage server and the backup storage server resides at a single site. You can distribute application servers at different locations. Application servers are shared by both the storage servers.


Telephony
Cluster
Application Server 1
10.200.0.1
Application Server 2
10.200.0.2
Network
Telephony
Application Server 3
10.200.0.3
Site B
Storage Server 1
(Primary)
Mutare Server
Storage Server 2
(Backup)
Site A
Telephony
Cluster
Application Server 1
10.200.0.1
Application Server 2
10.200.0.2
Network
Telephony
Application Server 3
10.200.0.3
Storage Server 1
(Primary)
Mutare Server
Site A
Storage Server 2
(Backup)
Site B

The following are examples of the topology page configuration.

Example

Initial setup of a new mirrored Messaging system.



Failover service to the backup Messaging system.



(If primary storage server is accessible)

Failback service to the primary Messaging system.



Caveats

You must use a Network Time Protocol (NTP) server within your network to synchronize the time of the System Platform server. The Avaya message store server and the Message Mirror server must synchronize with the NTP server.

Message Mirror does not replicate the following:

- System broadcast messages
- System lists such as ELAs and PDLs
- Messages stored in a folder other than the Inbox folder
- Future delivery messages that are stored in a queue
- Application layer data, including sites and topology
- Administrative logins

- Nightly backup schedule
- Certificates

Messaging does not support Message Mirror when:

- the application server and the storage server are active on the same server, that is a single server configuration.
- the single server configuration has additional application servers.
- all application servers are not duplicated.
- the Microsoft Exchange server is used as a message storage server.

Planning and preconfigurations

Messaging Hardware and Software requirements

Hardware requirements

- Both the primary Messaging system and the backup Messaging system must run the HP DL360 G7, Dell™ PowerEdge™ R610, S8800 1U, or S8730 servers.
- The hardware configuration including all physical LAN connections of the backup Messaging system must be identical to the hardware configuration of the primary system.

Software requirements

- Both the primary Messaging system and the backup Messaging system must run Messaging 6.2 or later.
- The software configuration of the backup Messaging system, including all updates and patches, must be identical to the software configuration of the primary system.
- The set of language packs must be identical on both the primary Messaging system and the backup Messaging system.

License requirements

A Messaging system with Mutare Message Mirror needs a dual host license. You must provide the WebLM host ID of primary and backup storage servers to activate the license file in PLDS.

The WebLM host ID is the MAC address of the server. You can obtain the WebLM host ID from the WebLM Web interface.

You must install the dual host license to both primary and backup storage servers. You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

Mutare Message Mirror requirements

Server hardware specifications

Names of components	Minimum specifications
Processor	2.8 GHz or faster processor; dual-core
System memory	4 GB
Disk	30 GB hard drive minimum space available
Ethernet connection	100 Mbps NIC for Ethernet connection to TCP/IP LAN

Server software requirements

- Any of the below listed server
  - Microsoft Windows Server 2003
  - Microsoft Windows Server 2008
  - Microsoft Windows Server 2008 R2
- Microsoft Internet Information Server 6.0 or 7.0.
  - SMTP Virtual Server to send Alarms and Status to System Admin.
  - Web Server for Mailbox Administration and View Status Reports and Errors
- Remote access - VPN Access to network and Remote Desktop to server.

Configuration information

Configuration information for primary Messaging system

To record the primary Messaging system information, print the following table and work with your network administrator to fill the empty cells.

Server	Host name	Msg IPv4 address	Notes
Storage server			
Application server 1			
Application server 2			
Application server 3			
Application server 4			

Configuration information for backup Messaging system

To record the backup Messaging system information, print the following table and work with your network administrator to fill the empty cells.

Server	Host name	Msg IPv4 address	Notes
Storage server			
Application server 1			
Application server 2			
Application server 3			
Application server 4			

Checklists

Checklist for duplicated application server configuration

Initial setup of a new mirrored Messaging system

Use the following checklist as a guide to set up a new mirrored Messaging system with duplicated application servers.

Complete the tasks in the sequence that is listed in the checklist.

Installing a primary Messaging system

	Server or System	Task	Required action
1	—	Install a primary Messaging system. For more information, see *Implementing Avaya Aura® Messaging*.	• Install System Platform with the latest patches and service packs verified with Messaging. • Install Messaging. • Install Communication Manager and Messaging patches.
2	—	Add a SIP trunk group to each primary application server. For more information, see switch configuration notes.	—
3	—	Configure a route pattern. For more information, see switch configuration notes.	—

Configuring the primary Messaging system

	Server or System	Task	Required action
1	Primary application server	For each application server, configure the switch link parameters of the Messaging system.	—

Comments? infodev@avaya.com

	Server or System	Task	Required action
		For more information, see Integrating with the telephony server on page 60.	
2	Primary application server	For each application server, configure the IP address of the primary storage server. For more information, see Changing the AxC IP address on page 70.	In the **AxC IP address** field, enter the IP address of the primary storage server.
3	Primary application server	Backup application files. For more information, see Backing up application files on page 72.	Select **Messaging Application** from the **Messaging** check box.
4	Primary storage server	Add application servers. For more information, see • Adding the first application server on page 96. • Adding additional application servers on page 97.	• From the **Add Application Server** heading, in the IP address field, enter the IP address of the application server you are joining to the cluster. • In the **Sites / Application Servers** table, select **Active** from the drop-down list.
5	Primary storage server	Set up the storage server networking with remote Messaging systems. **Note:** Perform this step only if you have a Remote Messaging system. For more information, see Setting up remote updates on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.
6	Primary storage server	Add remote systems as a networked server. **Note:** Perform this step only if you have a Remote Messaging system. For more information, see • Adding a network server on page 113. • Setting up remote updates on page 153.	• Add the remote systems • Set the **Updates In** and **Updates Out** fields to **yes**.

	Server or System	Task	Required action
7	Remote systems	Add the primary storage server as a networked server. **Note:** Perform this step only if you have a Remote Messaging system. For more information, see • Adding a network server on page 113. • Setting up remote updates on page 153.	• Add the primary storage server. • Set the **Updates In** and **Updates Out** fields to **yes**.
8	Primary storage server	Request update for each remote system. For more information, see Running a remote update manually on page 153.	On the Request Remote Update Web page, select remote system from the drop-down list.
9	Primary application server	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.
10	Remote system	Request update for the primary storage server. For more information, see Running a remote update manually on page 153.	On the Request Remote Update Web page, select **primary storage server** from the drop-down list.
11	Remote system	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Installing a backup application server

	Server or System	Task	Required action
1	—	Install a backup application server. For more information, see *Implementing Avaya Aura® Messaging*.	• Install System Platform with the latest patches and service packs verified with Messaging. • Install Messaging. • Install Communication Manager and Messaging patches.

	Server or System	Task	Required action
2	—	Add a SIP trunk group to each primary application server. For more information, see switch configuration notes.	Disable call routing to the backup application servers so that all calls route to only primary application servers.

Configuring the backup application server

	Server or System	Task	Required action
1	Backup application server	Restore data that you backed up from the backup of primary server. For more information, see Performing a restore on page 221.	Restore *Messaging Application, audix*.gz*.
2	Backup application server	For each application server, configure the switch link parameters of the Messaging system. For more information, see Integrating with the telephony server on page 60.	—
3	Backup application server	For each application server, configure the IP address of the backup storage server. For more information, see Changing the AxC IP address on page 70.	In the **AxC IP address** field, enter the IP address of the backup storage server.

Configuring the primary storage server

	Server or System	Task	Required action
1	Primary storage server	Add backup application servers. For more information, see • Adding the first application server on page 96. • Adding additional application servers on page 97.	• From the **Add Application Server** heading, in the IP address field, enter the IP address of the backup application server you are joining to the cluster. • In the **Sites / Application Servers** table, select **Inactive** from the drop-down list.

	Server or System	Task	Required action
2	Primary storage server	Verify that the storage server is configured as a primary server. For more information, see Changing the storage server role on page 99.	From the **Role of the Server** heading, verify that the storage server role is **Primary**. **Note:** The system applies MWIs and LDAP updates to all application servers after you make storage server as the primary server.
3	Primary storage server	Add a new Message Mirror server as a trusted server. For more information, see Adding a trusted server on page 105.	• In the **Trusted Server Name** field, enter an appropriate name for the Message Mirror server. The trusted server name must correspond to the **Super User** name you configured on the Message Mirror Admin page. • In the **Password** field, enter the password that server uses to connect to Messaging. The password must correspond to the **Super Pwd** password you configured on the Message Mirror Admin page. • In the **Machine Name / IP Address** field, enter the host name or the valid IP address of the Message Mirror server. • Set **LDAP Access Allowed** to **yes**. • Set **IMAP4 Super User Access Allowed** to **yes**.
4	Primary storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. For more information, see Configuring the mail options on page 307.	• If the alias configured for both primary and backup storage servers in DNS is identical, add the alias to the **Server Alias** field. • If not, leave the **Server Alias** field blank.
5	System Platform Web Console of primary	Backup theSystem Platform Web Console configuration data. For more information, see Backing up System Platform on page 216.	On the Backup page, select the **Backup Now** option to start the backup operation immediately.

	Server or System	Task	Required action
	storage server		
6	Primary storage server	Backup application files. For more information, see Backing up application files on page 72.	• Stop Messaging. • Select **Messaging Application and Translations** from the **Messaging** check box. • Start Messaging.

Install a backup storage server

	Server or System	Task	Required action
1	—	Install a backup storage server. For more information, see *Implementing Avaya Aura® Messaging*.	• Install System Platform with the latest patches and service packs verified with Messaging. • Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the backup storage server

	Server or System	Task	Required action
1	System Platform Web Console of backup storage server	Restore theSystem Platform Web Console configuration data. For more information, see • Restoring System Platform configuration information on page 225. • Viewing restore history on page 226.	• Restore *System Platform Web Console, backup*cdom*.tgz*. • Verify that restore status is `Success`.
2	Backup storage server	Restore data that you backed up from the backup of primary storage server.	• Stop Messaging. • Restore *Messaging Application, audix*.gz*. • Start Messaging.

	Server or System	Task	Required action
		For more information, see • Stopping Messaging on page 377. • Performing a restore on page 221. • Starting Messaging on page 377.	
3	Backup storage server	Configure the storage server as a backup server. For more information, see Changing the storage server role on page 99.	• From the **Role of the Server** heading, select **Backup**. **Note:** The system prevents MWIs and LDAP updates to all application servers after you make storage server as the backup server. • In the **Sites / Application Servers** table, select **Active** from the drop-down list for each backup application server. • In the **Sites / Application Servers** table, select **Inactive** from drop down for each primary application server.
4	Backup storage server	Verify that storage server is set to a backup server.	From the topology page and site page, verify the following: • Storage server role is set to Backup. • For each backup application server, status is set to Active. • For each primary application server, status is set to Inactive.
5	Backup storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. For more information, see Configuring the mail options on page 307.	• If the alias configured for both primary and backup storage servers in DNS is identical, add the alias to the **Server Alias** field. • If not, enter the Fully Qualified Domain Name (FQDN) of the

	Server or System	Task	Required action
			primary storage server in the **Server Alias** field.

Setting up a networked Messaging system

	Server or System	Task	Required action
1	Backup storage server	Set up storage server networking with remote Messaging systems. For more information, see Setting up remote updates on page 153.	Set the **Updates In** field to **yes** and **Updates Out** field to **no**.

Installing a license

Note:

You must install the dual host license to both the primary and backup storage servers. You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

	Server or System	Task	Required action
1	System Platform Web Console of the primary storage server	Install a license for the primary storage server. For more information, see *Implementing Avaya Aura® Messaging*.	—
2	System Platform Web Console of the backup storage server	Install a license for the backup storage server. For more information, see *Implementing Avaya Aura® Messaging*.	—

Backing up storage server

	Server or System	Task	Required action
1	Backup storage server	Backup storage server. For more information, see Backing up system files on page 213.	—

Configuring Mutare Message Mirror

	Server or System	Task	Required action
1	Message Mirror Admin interface	Configure Mutare Message Mirror For more information, see the Mutare Software product documentation.	—

Failover service to the backup Messaging system

Use the following checklist as a guide to switch service to the backup Messaging system with duplicated application servers.

Complete the tasks in the sequence that is listed in the checklist.

Changing DNS IP address

	Server or System	Task	Required action
1	—	Change DNS IP address alias from the primary storage server to the backup storage server.	—

Disabling Mirror

	Server or System	Task	Required action
1	Message Mirror Admin interface	Disable Mirror. For more information, see the Mutare Software product documentation.	—

Configuring the primary storage server as inactive

Note:

Perform this step only if the primary storage server is accessible.

	Server or System	Task	Required action
1	Primary storage server	Configure the primary storage server as a backup server.	From the **Role of the Server** heading, select **Backup**.

	Server or System	Task	Required action
		For more information, see Changing the storage server role on page 99.	**Note:** The system prevents MWIs and LDAP updates to all application servers after you make storage server as the backup server.
2	Primary storage server	Verify that the storage server is configured as a backup server. For more information, see Changing the storage server role on page 99.	From the topology page, verify that the storage server role is set to Backup.
3	Primary storage server	Set up storage server networking with remote Messaging systems. Fore more information, see Setting up remote updates on page 153.	• On the Manage Networked Servers Web page, select **remote system** and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **no**.
4	Primary storage server	Stop Messaging. For more information, see Stopping Messaging on page 377.	—

Changing the AxC address

	Server or System	Task	Required action
1	Primary application server.	Change the AxC address. You must change the AxC IP address to point to the new primary storage server so that: • The system pushes messages collected during the offline mode to the new primary storage server. • The system clears and reloads a user list and GAL. For more information, see Changing the AxC IP address on page 70.	In the **AxC IP address** field, enter the IP address of the new primary storage server.

Configuring the backup storage server as active

	Server or System	Task	Required action
1	Backup storage server	Configure the backup storage server as a primary server. For more information, see Changing the storage server role on page 99.	From the **Role of the Server** heading, select **Primary**. **Note:** The system prevents MWIs and LDAP updates to all application servers after you make storage server as the backup server.
2	Backup storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. **Note:** Perform this step if DNS IP address alias is not changed from primary storage server to backup storage server during failover. For more information, see Configuring the mail options on page 307.	• If the alias configured for both primary and backup storage servers in DNS is identical, add the alias to the **Server Alias** field. • If not, leave the **Server Alias** field blank.
3	Backup storage server	Set up storage server networking with remote messaging systems. For more information, see Setting up remote updates on page 153.	• On the Manage Networked Servers Web page, select **remote system** and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **yes**.
4	Backup storage server	Stop Messaging. For more information, see Stopping Messaging on page 377.	—
5	Backup storage server	Start Messaging. For more information, see Starting Messaging on page 377.	—

Reloading User List and Global Address List

	Server or System	Task	Required action
1	Backup application server	Reload User List and Global Address List.	• On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**. • From the **Reload Caches** heading: - Click **Reload** next to the **User List** field to load the User List. - Click **Reload** next to the **Global Address List** field to load the Global Address List.

Removing application server trunk groups

	Server or System	Task	Required action
1	—	Remove all active application server trunk groups. For more information, see switch configuration notes.	—
2	—	Add all backup application server trunk groups For more information, see switch configuration notes.	Disable call routing to the primary application servers so that all calls route to only backup application servers.

Running diagnostic test

	Server or System	Task	Required action
1	Primary application server	Run test to ensure that all offline messages are delivered to the new primary storage server. **Note:** The test can take up to 10 minutes for all calling functions. For more information, see Running application server diagnostics on page 337.	• From the **Select the test(s) to run** down list, select **Messages to Deliver**. • Click **Run Tests** periodically until **Voicemails to send** is 0.

Changing the AxC address

	Server or System	Task	Required action
1	Primary application server	Change the AxC address. **Note:** You must change the AxC IP address to point to the previous primary storage server. For more information, see Changing the AxC IP address on page 70.	In the **AxC IP address** field, enter the IP address of the primary storage server.

Configuring remote Messaging systems

	Server or System	Task	Required action
1	Remote system	Configure the primary storage server as a networked server. For more information, see Adding a network server on page 113.	On the Manage Networked Server web page, change the value for the following fields: • Hostname • IP address • Password
2	Remote system	Request update for the backup storage server. For more information, see Running a remote update manually on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.
3	Remote system	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Requesting updates for backup storage server

	Server or System	Task	Required action
1	Backup storage server	Request update for the remote system. For more information, see Running a remote update manually on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.

	Server or System	Task	Required action
2	Backup storage server	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Failback service to the primary Messaging system

Use the following checklist as a guide to return service to the primary Messaging system with duplicated application servers.

Important:

Perform the following tasks only during a planned downtime for system maintenance.

Complete the tasks in the sequence that is listed in the checklist.

Disabling routing of calls

	Server or System	Task	Required action
1	—	Disable routing of calls to application servers For more information, see switch configuration notes.	—

Changing DNS IP address

	Server or System	Task	Required action
1	—	Change DNS IP address alias from backup storage server to primary storage server.	—

Configuring the backup storage server as inactive

	Server or System	Task	Required action
1	System Platform Web Console of backup	Backup theSystem Platform Web Console configuration data. For more information, see Backing up System Platform on page 216.	On the Backup page, select the **Backup Now** option to start the backup operation immediately.

	Server or System	Task	Required action
	storage server		
2	Backup storage server	Backup application files. For more information, see Backing up application files on page 72.	• Stop Messaging. • Select **Messaging Application, Translations, Names, and Messages** from the **Messaging** check box. • Start Messaging.
3	Backup storage server	Configure the storage server as a backup server. For more information, see Changing the storage server role on page 99.	From the **Role of the Server** heading, select **Backup**. **Note:** The system prevents MWIs and LDAP updates to all application servers after you make storage server as the backup server.
4	Backup storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. **Note:** Perform this step if DNS IP address alias is not changed from primary storage server to backup storage server during failover. For more information, see Configuring the mail options on page 307.	Add primary storage server alias in the **Server Alias** field.
5	Backup storage server	Set up storage server networking with remote Messaging systems. For more information, see Setting up remote updates on page 153.	• On the Manage Networked Servers Web page, select **remote system** and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **no**.
6	Backup storage server	Stop Messaging. For more information, see Stopping Messaging on page 377.	—

	Server or System	Task	Required action
7	Backup storage server	Start Messaging. For more information, see Starting Messaging on page 377.	—

Installing a primary storage server

	Server or System	Task	Required action
1	Primary storage server	Install a primary storage server. For more information, see *Implementing Avaya Aura® Messaging*.	• Install System Platform with the latest patches and service packs verified with Messaging. • Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the primary storage server

	Server or System	Task	Required action
1	System Platform Web Console of primary storage server	Restore theSystem Platform Web Console configuration data. For more information, see • Restoring System Platform configuration information on page 225. • Viewing restore history on page 226.	• Restore *System Platform Web Console, backup*cdom*.tgz*. • Verify that restore status is `Success`.
2	Primary storage server	Restore data that you backed up during step *2b* from the backup of primary storage server. For more information, see • Stopping Messaging on page 377. • Performing a restore on page 221. • Starting Messaging on page 377.	• Stop Messaging. • Restore *Messaging Application, audix*.gz*. • Start Messaging.
3	Primary storage server	Configure the primary storage server as active.	• In the **Sites / Application Servers** table, select **Active** from

	Server or System	Task	Required action
			the drop-down list for each primary application server. • In the **Sites / Application Servers** table, select **Inactive** from the drop-down list for each backup application server. • Click **Update**.
4	Primary storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. For more information, see Configuring the mail options on page 307.	• If the alias configured for both primary and backup storage servers in DNS is identical, add the alias to the **Server Alias** field. • If not, leave the **Server Alias** field blank.

Changing the AxC address

	Server or System	Task	Required action
1	Primary application server	Change the AxC address. For more information, see Changing the AxC IP address on page 70.	In the **AxC IP address** field, enter the IP address of the primary storage server.
2	Primary application server	Reload User List and Global Address List.	• On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**. • From the **Reload Caches** heading: - Click **Reload** next to the **User List** field to load the User List. - Click **Reload** next to the **Global Address List** field to load the Global Address List.

Configuring remote Messaging systems

	Server or System	Task	Required action
1	Remote system	Configure the storage server from backup to primary. For more information, see Adding a network server on page 113.	On the Manage Networked Server web page, change the value for the following fields: • Hostname • IP address • Password
2	Remote system	Request update for the primary storage server. For more information, see Running a remote update manually on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.
3	Remote system	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Requesting updates for primary storage server

	Server or System	Task	Required action
1	Primary storage server	Request update for the remote system. For more information, see Running a remote update manually on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.
2	Primary storage server	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Installing a license

	Server or System	Task	Required action
1	System Platform Web Console of the primary	Install a license for the primary storage server. For more information, see *Implementing Avaya Aura® Messaging*.	—

	Server or System	Task	Required action
	storage server		

Enabling Mirror

	Server or System	Task	Required action
1	Message Mirror Admin interface	Enable Mirror. For more information, see the Mutare Software product documentation.	—

Enabling call routing

	Server or System	Task	Required action
1	—	Enable routing of calls to all primary application servers. For more information, see switch configuration notes.	—

Checklist for shared application server configuration

Initial setup of a new mirrored Messaging system

Use the following checklist as a guide to set up a new mirrored Messaging system with shared application servers.

Complete the tasks in the sequence that is listed in the checklist.

Installing a primary Messaging system

	Server or System	Task	Required action
1	—	Install a primary Messaging system. For more information, see *Implementing Avaya Aura® Messaging*.	• Install System Platform with the latest patches and service packs verified with Messaging. • Install Messaging. • Install Communication Manager and Messaging patches.
2	—	Add a SIP trunk group to each primary application server. For more information, see switch configuration notes.	—
3	—	Configure a route pattern. For more information, see switch configuration notes.	—

Configuring the primary Messaging system

	Server or System	Task	Required action
1	Application server	For each application server, configure the switch link parameters of the Messaging system. For more information, see Integrating with the telephony server on page 60.	—
2	Application server	For each application server, configure the IP address of the primary storage server. For more information, see Changing the AxC IP address on page 70.	In the **AxC IP address** field, enter the IP address of the primary storage server.
3	Primary storage server	Add application servers. For more information, see • Adding the first application server on page 96. • Adding additional application servers on page 97.	• From the **Add Application Server** heading, in the IP address field, enter the IP address of the application server you are joining to the cluster. • In the **Sites / Application Servers** table, select **Active** from the drop-down list.

	Server or System	Task	Required action
4	Primary storage server	Set up the storage server networking with remote Messaging systems. **Note:** Perform this step only if you have a Remote Messaging system. For more information, see Setting up remote updates on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.
5	Primary storage server	Add remote systems as a networked server. **Note:** Perform this step only if you have a Remote Messaging system. For more information, see • Adding a network server on page 113. • Setting up remote updates on page 153.	• Add the remote systems • Set the **Updates In** and **Updates Out** fields to **yes**.
6	Remote systems	Add the primary storage server as a networked server. **Note:** Perform this step only if you have a Remote Messaging system. For more information, see • Adding a network server on page 113. • Setting up remote updates on page 153.	• Add the primary storage server. • Set the **Updates In** and **Updates Out** fields to **yes**.
7	Primary storage server	Request update for each remote system. For more information, see Running a remote update manually on page 153.	On the Request Remote Update Web page, select remote system from the drop-down list.
8	Application server	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

	Server or System	Task	Required action
9	Remote system	Request update for the primary storage server. For more information, see Running a remote update manually on page 153.	On the Request Remote Update Web page, select **primary storage server** from the drop-down list.
10	Remote system	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Configuring the primary storage server

	Server or System	Task	Required action
1	Primary storage server	Verify that the storage server is configured as a primary server. For more information, see Changing the storage server role on page 99.	From the **Role of the Server** heading, verify that the storage server role is **Primary**. **Note:** The system applies MWIs and LDAP updates to all application servers after you make storage server as the primary server.
2	Primary storage server	Add a new Message Mirror server as a trusted server. For more information, see Adding a trusted server on page 105.	• In the **Trusted Server Name** field, enter an appropriate name for the Message Mirror server. The trusted server name must correspond to the **Super User** name you configured on the Message Mirror Admin page. • In the **Password** field, enter the password that server uses to connect to Messaging. The password must correspond to the **Super Pwd** password you configured on the Message Mirror Admin page. • In the **Machine Name / IP Address** field, enter the host name or the valid IP address of the Message Mirror server.

	Server or System	Task	Required action
			• Set **LDAP Access Allowed** to **yes**. • Set **IMAP4 Super User Access Allowed** to **yes**.
3	Primary storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. For more information, see Configuring the mail options on page 307.	• If the alias configured for both primary and backup storage servers in DNS is identical, add the alias to the **Server Alias** field. • If not, leave the **Server Alias** field blank.
4	System Platform Web Console of primary storage server	Backup theSystem Platform Web Console configuration data. For more information, see Backing up System Platform on page 216.	On the Backup page, select the **Backup Now** option to start the backup operation immediately.
5	Primary storage server	Backup application files. For more information, see Backing up application files on page 72.	Select **Messaging Application and Translations** from the **Messaging** check box.

Installing a backup storage server

	Server or System	Task	Required action
1	—	Install a backup storage server. For more information, see *Implementing Avaya Aura® Messaging*.	• Install System Platform with the latest patches and service packs verified with Messaging. • Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the backup storage server

	Server or System	Task	Required action
1	System Platform Web Console of backup storage server	Restore theSystem Platform Web Console configuration data. For more information, see • Restoring System Platform configuration information on page 225. • Viewing restore history on page 226.	• Restore *System Platform Web Console, backup*cdom*.tgz*. • Verify that restore status is `Success`.
2	Backup storage server	Restore data that you backed up from the backup of primary storage server. For more information, see • Stopping Messaging on page 377. • Performing a restore on page 221. • Starting Messaging on page 377.	• Stop Messaging. • Restore *Messaging Application, audix*.gz*. • Start Messaging.
3	Backup storage server	Configure the storage server as a backup server. For more information, see Changing the storage server role on page 99.	• From the **Role of the Server** heading, select **Backup**. **Note:** The system prevents MWIs and LDAP updates to all application servers after you make storage server as the backup server. • In the **Sites / Application Servers** table, select **Shared** from the drop-down list for each application server.

	Server or System	Task	Required action
4	Backup storage server	Verify that storage server is set to a backup server.	From the topology page and site page, verify the following: • Storage server role is set to Backup. • For each backup application server, status is set to Active. • For each primary application server, status is set to Inactive.
5	Backup storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. For more information, see Configuring the mail options on page 307.	• If the alias configured for both primary and backup storage servers in DNS is identical, add the alias to the **Server Alias** field. • If not, enter the Fully Qualified Domain Name (FQDN) of the primary storage server in the **Server Alias** field.

Setting up a networked Messaging system

	Server or System	Task	Required action
1	Backup storage server	Set up storage server networking with remote Messaging systems. For more information, see Setting up remote updates on page 153.	Set the **Updates In** field to **yes** and **Updates Out** field to **no**.

Installing a license

Note:

You must install the dual host license to both the primary and backup storage servers. You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

	Server or System	Task	Required action
1	System Platform Web Console of the primary	Install a license for the primary storage server. For more information, see *Implementing Avaya Aura® Messaging*.	—

	Server or System	Task	Required action
	storage server		
2	System Platform Web Console of the backup storage server	Install a license for the backup storage server. For more information, see *Implementing Avaya Aura® Messaging*.	—

Backing up storage server

	Server or System	Task	Required action
1	Backup storage server	Backup storage server. For more information, see Backing up system files on page 213.	—

Configuring Mutare Message Mirror

	Server or System	Task	Required action
1	Message Mirror Admin interface	Configure Mutare Message Mirror For more information, see the Mutare Software product documentation.	—

Failover service to the backup Messaging system

Use the following checklist as a guide to switch service to the backup Messaging system with shared application servers.

Complete the tasks in the sequence that is listed in the checklist.

Changing DNS IP address

	Server or System	Task	Required action
1	—	Change DNS IP address alias from the primary storage server to the backup storage server.	—

Disabling Mirror

	Server or System	Task	Required action
1	Message Mirror Admin interface	Disable Mirror. For more information, see the Mutare Software product documentation.	—

Configuring the primary storage server as inactive

Note:

Perform this step only if the primary storage server is accessible.

	Server or System	Task	Required action
1	Primary storage server	Configure the primary storage server as a backup server. For more information, see Changing the storage server role on page 99.	• From the **Role of the Server** heading, select **Backup**. • In the **Sites / Application Servers** table, select **Shared** from the drop-down list next to the site.
2	Primary storage server	Verify that the storage server is configured as a backup server. For more information, see Changing the storage server role on page 99.	From the topology page, verify that the storage server role is set to Backup.
3	Primary storage server	Set up storage server networking with remote Messaging systems. Fore more information, see Setting up remote updates on page 153.	• On the Manage Networked Servers Web page, select **remote system** and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **no**.
4	Primary storage server	Stop Messaging. For more information, see Stopping Messaging on page 377.	—

Changing the AxC address

	Server or System	Task	Required action
1	Application server.	Change the AxC address. You must change the AxC IP address to point to the new primary storage server so that: • The system pushes messages collected during the offline mode to the new primary storage server. • The system clears and reloads a user list and GAL. For more information, see Changing the AxC IP address on page 70.	In the **AxC IP address** field, enter the IP address of the new primary storage server.

Configuring the backup storage server as active

	Server or System	Task	Required action
1	Backup storage server	Configure the backup storage server as a primary server. For more information, see Changing the storage server role on page 99.	• In the **Sites / Application Servers** table, select **Active** from the drop-down list next to the site. • From the **Role of the Server** heading, select **Primary**.
2	Backup storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. **Note:** Perform this step if DNS IP address alias is not changed from primary storage server to backup storage server during failover. For more information, see Configuring the mail options on page 307.	• If the alias configured for both primary and backup storage servers in DNS is identical, add the alias to the **Server Alias** field. • If not, leave the **Server Alias** field blank.

	Server or System	Task	Required action
3	Backup storage server	Set up storage server networking with remote messaging systems. For more information, see Setting up remote updates on page 153.	• On the Manage Networked Servers Web page, select **remote system** and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **yes**.
4	Backup storage server	Stop Messaging. For more information, see Stopping Messaging on page 377.	—
5	Backup storage server	Start Messaging. For more information, see Starting Messaging on page 377.	—

Reloading application server cache

	Server or System	Task	Required action
1	Application server	Clear greetings from ADCS cache.	• On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**. • From the **Distributed Cache (ADCS) Maintenance** heading, click **Clear Greetings/Names** to clear all greetings and names in ADCS cache on this application server.
2	Application server	Reload User List and Global Address List.	• On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**. • From the **Reload Caches** heading: - Click **Reload** next to the **User List** field to load the User List. - Click **Reload** next to the **Global Address List** field to load the Global Address List.

Configuring remote Messaging systems

	Server or System	Task	Required action
1	Remote system	Configure the primary storage server as a networked server. For more information, see Adding a network server on page 113.	On the Manage Networked Server web page, change the value for the following fields: • Hostname • IP address • Password
2	Remote system	Request update for the backup storage server. For more information, see Running a remote update manually on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.
3	Remote system	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Requesting updates for backup storage server

	Server or System	Task	Required action
1	Backup storage server	Request update for the remote system. For more information, see Running a remote update manually on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.
2	Backup storage server	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Failback service to the primary Messaging system

Use the following checklist as a guide to return service to the primary Messaging system with shared application servers.

Important:

Perform the following tasks only during a planned downtime for system maintenance.

Complete the tasks in the sequence that is listed in the checklist.

Disabling routing of calls

	Server or System	Task	Required action
1	—	Disable routing of calls to application servers For more information, see switch configuration notes.	—

Changing DNS IP address

	Server or System	Task	Required action
1	—	Change DNS IP address alias from backup storage server to primary storage server.	—

Configuring the backup storage server as inactive

	Server or System	Task	Required action
1	System Platform Web Console of backup storage server	Backup theSystem Platform Web Console configuration data. For more information, see Backing up System Platform on page 216.	On the Backup page, select the **Backup Now** option to start the backup operation immediately.
2	Backup storage server	Backup application files. For more information, see Backing up application files on page 72.	• Stop Messaging. • Select **Messaging Application, Translations, Names, and Messages** from the **Messaging** check box. • Start Messaging.
3	Backup storage server	Configure the storage server as a backup server. For more information, see Changing the storage server role on page 99.	• From the **Role of the Server** heading, select **Backup**. **Note:** The system prevents MWIs and LDAP updates to all application servers after you

	Server or System	Task	Required action
			make storage server as the backup server. • In the **Sites / Application Servers** table, select **Shared** from the drop-down list for each application server.
4	Backup storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. **Note:** Perform this step if DNS IP address alias is not changed from primary storage server to backup storage server during failover. For more information, see Configuring the mail options on page 307.	Add primary storage server alias in the **Server Alias** field.
5	Backup storage server	Set up storage server networking with remote Messaging systems. For more information, see Setting up remote updates on page 153.	• On the Manage Networked Servers Web page, select **remote system** and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **no**.
6	Backup storage server	Stop Messaging. For more information, see Stopping Messaging on page 377.	—
7	Backup storage server	Start Messaging. For more information, see Starting Messaging on page 377.	—

Installing a primary storage server

	Server or System	Task	Required action
1	Primary storage server	Install a primary storage server. For more information, see *Implementing Avaya Aura® Messaging*.	• Install System Platform with the latest patches and service packs verified with Messaging. • Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the primary storage server

	Server or System	Task	Required action
1	System Platform Web Console of primary storage server	Restore theSystem Platform Web Console configuration data. For more information, see • Restoring System Platform configuration information on page 225. • Viewing restore history on page 226.	• Restore *System Platform Web Console, backup*cdom*.tgz*. • Verify that restore status is `Success`.
2	Primary storage server	Restore data that you backed up during step *2b* from the backup of primary storage server. For more information, see • Stopping Messaging on page 377. • Performing a restore on page 221. • Starting Messaging on page 377.	• Stop Messaging. • Restore *Messaging Application, audix*.gz*. • Start Messaging.
3	Primary storage server	Configure the mail options. Configuring the mail options facilitates delivery of messages collected in the offline mode, that is, in a failover. For more information, see Configuring the mail options on page 307.	• If the alias configured for both primary and backup storage servers in DNS is identical, add the alias to the **Server Alias** field. • If not, leave the **Server Alias** field blank.

	Server or System	Task	Required action
4	Primary storage server	Start Messaging. For more information, see Starting Messaging on page 377.	—

Changing the AxC address

	Server or System	Task	Required action
1	Primary application server	Change the AxC address. For more information, see Changing the AxC IP address on page 70.	In the **AxC IP address** field, enter the IP address of the primary storage server.
2	Primary application server	Reload User List and Global Address List.	• On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**. • From the **Reload Caches** heading: - Click **Reload** next to the **User List** field to load the User List. - Click **Reload** next to the **Global Address List** field to load the Global Address List.

Configuring remote Messaging systems

	Server or System	Task	Required action
1	Remote system	Configure the storage server from backup to primary. For more information, see Adding a network server on page 113.	On the Manage Networked Server web page, change the value for the following fields: • Hostname • IP address • Password
2	Remote system	Request update for the primary storage server. For more information, see Running a remote update manually on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.

	Server or System	Task	Required action
3	Remote system	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Requesting updates for primary storage server

	Server or System	Task	Required action
1	Primary storage server	Request update for the remote system. For more information, see Running a remote update manually on page 153.	Set the **Updates In** and **Updates Out** fields to **yes**.
2	Primary storage server	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 175.	To load the Global Address List, click **Reload Caches** > **Reload**.

Installing a license

	Server or System	Task	Required action
1	System Platform Web Console of the primary storage server	Install a license for the primary storage server. For more information, see *Implementing Avaya Aura® Messaging*.	—

Enabling Mirror

	Server or System	Task	Required action
1	Message Mirror Admin interface	Enable Mirror. For more information, see the Mutare Software product documentation.	—

Enabling call routing

	Server or System	Task	Required action
1	—	Enable routing of calls to all primary application servers. For more information, see switch configuration notes.	—

Validating the configuration

This topic outlines a procedure for validating the message store redundancy configuration.

Tasks	Server	Steps	Result / Validate
Create test users.	Primary storage server	Add the following test users: • Create Test User 1. • Create Test User 2. For more information, see Adding users on page 134.	
Check whether test users are added to the primary storage server.	Primary storage server	Click **Messaging** > **Reports (Storage)** > **Users**. For more information, see Viewing the local users report on page 278.	Test users added to the primary storage server.
	Primary application server	• Click **Messaging** > **Diagnostics** > **Diagnostics (Application)**. • From the **Select the test(s) to run** field, select **User and Contact Lists**. For more information, see Running application server diagnostics on page 337	

Tasks	Server	Steps	Result / Validate
Check whether test users added to the primary storage server are mirrored to the backup storage server. **Note:** Users are mirrored every one hour, so you must wait for one hour before you perform this step.	Backup storage server	Click **Messaging** > **Reports (Storage)** > **Users**. For more information, see Viewing the local users report on page 278.	Test users added to the primary storage server are mirrored to the backup storage server.
	Backup application server	• Click **Messaging** > **Diagnostics** > **Diagnostics (Application)**. • From the **Select the test(s) to run** field, select **User and Contact Lists**. For more information, see Running application server diagnostics on page 337	
Basic call answer.	Backup system through Outlook toolbar	Perform the following: • From extension of Test User2, call direct extension number for Test User1 and let the call roll over to voice mail. • Leave a message; note user details, and date and time when the message is sent. • Hangup. For more information, see the *Using Avaya Aura® Messaging* guide.	
Check voice messages. **Note:** Messages are mirrored every one minute, so you must wait for one minute before you perform this step.	Backup system through Outlook toolbar	Perform the following: • As Test User1, log in to the IMAP account using Outlook and inspect voice messages. • Use Play on PC for a message. • Use Play on Phone for a message.	Observe the following: • The system plays the message using the media player for playing on PC. • The system plays the message using the TUI for playing on phone.

Tasks	Server	Steps	Result / Validate
		For more information, see the *Using Avaya Aura® Messaging* guide.	
(Optional) Perform configuration testing.		You can perform the following testing on primary and backup systems. • Configuration of remote users • Call routing	

Chapter 20: Troubleshooting

System cannot recognize the DTMF tones

After you install or upgrade Messaging, you might experience problems with the recognition of DTMF tones or while leaving voice mail messages. You might face these problems due to the ARP spoofing protection of the gateway.

Note:

This problem is only valid for G450 gateways and requires root access to the gateway. If you require assistance, consult Avaya Services.

Troubleshooting steps

Procedure

1. Start an SSH session on `<G450 IP Address>`.
2. Log in as `root`.
3. Enter the password for the root user.
4. After you log in successfully, type the following command.
   `clear arp-cache`

System drops call while logging in to the mailbox

When you log in to the mailbox, the Messaging system drops the call.

Troubleshooting steps

Procedure

On Avaya Aura® Session Border Controller (AASBC1), disable *third-party-call-control*.

For more information, see Avaya Aura® Session Border Controller.

System displays an error while performing a backup

When you start the backup process, the system displays an error message stating that Messaging cannot find few files.

Troubleshooting steps

Procedure

Check whether you are using a Network Time Protocol (NTP) or Point-to-Point Protocol (PPP) server.

The system displays the error message if you do not use the NTP or PPP server.

Tip:

Use the `cat os_ds.conf` command to view the files that the Messaging system backs up.

Application server does not recognize users

The application server does not recognize users.

Troubleshooting steps

If the application server does not recognize users, you must synchronize the cache on that application server.

Procedure

1. On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**.
2. To clear all data in the ADCS cache on the application server, click **Clear Cache**.
3. Restart Messaging for the changes to take effect.
   For more information, see Stopping on page 377 and Starting on page 377.
4. To reload the user list, click **Reload**.
5. To reload the global address list, click **Reload**.
6. To synchronize ADCS, click **Synchronize**.

Message is sent successfully but MWI does not turn on

The system sends the message successfully. However, the MWI does not turn on.

Troubleshooting steps

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **Diagnostics (Application)**.
2. From the **Select the test(s) to run** field, select **MWI**.
3. Enter the extension number of the user.
4. Click **Run Tests**.
   The system displays the test results or errors in the **Results** area.
   - If MWI lights during the test and the results indicate success, this indicates that Messaging works properly. However, you might have configured Communication Manager or Session Manager incorrectly.
   - If MWI does not light during the test and the results indicate failure, there might be a problem with Messaging or a connection issue between Messaging and Session Manager.
5. On the command prompt, view `InfoBridge.log` on application server to check if Messaging creates and sends MWI to extension.

6. On the command prompt, view `MWI.log` to check how the system routes the MWI message to Session Manager. You can then run a query on Session Manager to debug why the system does not route the MWI to extension.

Message does not reach recipient

You compose and send a message to an Exchange user. The system displays a message stating that it sent the message. However, the message does not reach the recipient.

Troubleshooting steps

Check the connection between the Microsoft Exchange server and the Messaging server.

Procedure

1. On the Exchange server at `\WINDOWS\system32\LogFiles\W3SVC1`, check if Messaging sends the request to the Exchange server.
2. On the Messaging command prompt, check `aic.log`.
3. In the `/VM/iim/logs` directory, check `smtp.log`.
4. To see if the Exchange server is working properly, check the CPU usage and memory of Exchange server .

Fax troubleshooting

In Messaging, faxes fail because of one or more of the missing basic provisioning requirements. To validate if you have implemented fax properly, see Implementing fax on page 66.

Fax error handling

- Condition: You have configured CoS for fax support. However, the fax email is unavailable.
  - Result: The system rejects the fax at transmission time.
- Condition: You have configured CoS for fax support. However, the fax email is unavailable and the AxC is offline.
  - Result: The system sends the fax to the postmaster account.
- Condition: You have configured an incorrect email address.
  - Result: The system sends the DSN to the postmaster account.

Appendix A: Changing the server role from storage and application to storage only

Use the following checklist to change the role of the server from storage and application to only storage.

For example, you have server A with a single-server configuration. Server A is a virtual machine that performs both roles: application and storage. You want to make the following changes:

- Add two more application servers: server B and server C.
- Ensure that server A performs the role of a storage server only.

No.	Task	Server or system	Required action
1	Install application servers.		
1a	Install application server B. For more information, see *Implementing Avaya Aura® Messaging*.		• Install System Platform with the latest patches and service packs verified for use with Messaging. • Install Messaging. • Install Communication Manager and Messaging patches.
1b	Install application server C. For more information, see *Implementing Avaya Aura® Messaging*.		• Install System Platform with the latest patches and service packs verified for use with Messaging. • Install Messaging. • Install Communication Manager and Messaging patches.
2	Add application servers.		
2a	Add server B as an application server.	Server B	In the **Add Application Server** area: • From the **Add the server with** heading, select **Same site configuration as an existing application server**. • From the **IP Address** drop-down menu, select the IP address of server A.

No.	Task	Server or system	Required action
2b	Add server C as an application server.	Server C	In the **Add Application Server** area: • From the **Add the server with** heading, select **Same site configuration as an existing application server**. • From the **IP Address** drop-down menu, select the IP address of server A.
3	For each application server, update the cluster configuration.		
3a	Define the application server C as a member of the cluster. For more information, see Configuring a cluster on page 99.	Server B	• In the **Number of member appliances in the cluster** field, enter 2. • In the **Member** field, enter the IP address of server C.
3b	Define the application server B as a member of the cluster. For more information, see Configuring a cluster on page 99.	Server C	• In the **Number of member appliances in the cluster** field, enter 2. • In the **Member** field, enter the IP address of server B.
4	For each application server, change the AxC address.		
4a	On application server B, change the AxC address. For more information, see Changing the AxC IP address on page 70.	Server B	In the **AxC IP address** field, enter the IP address of the server A.
4b	On application server C, change the AxC address. For more information, see Changing the AxC IP address on page 70.	Server C	In the **AxC IP address** field, enter the IP address of the server A.
5	Remove application server A.	Server A	• On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**. • From the **Remove Application Server** area, select the IP address of server A. • Click **Remove**.
6	Change Switch Integration. For more information, see Integrating with the telephony server on page 60.	Server A	From the **Switch Integration Type** drop-down, select **None**.

No.	Task	Server or system	Required action
7	Restart Messaging servers.		
7a	Restart server A. • For more information, see Stopping Messaging on page 377. • For more information, see Starting Messaging on page 377.	Server A	• Stop Messaging. • Start Messaging.
7b	Restart server B. • For more information, see Stopping Messaging on page 377. • For more information, see Starting Messaging on page 377.	Server B	• Stop Messaging. • Start Messaging.
7c	Restart server C. • For more information, see Stopping Messaging on page 377. • For more information, see Starting Messaging on page 377.	Server C	• Stop Messaging. • Start Messaging.
8	For each application server, reload User List and Global Address List Cache.		
8a	On server B, reload User List and Global Address List Cache. For more information, see Loading lists on page 175.	Server B	From the **Reload Caches** heading: • Click **Reload** next to the **User List** field to load the User List. • Click **Reload** next to the **Global Address List** field to load the Global Address List.
8b	On server C, reload User List and Global Address List Cache. For more information, see Loading lists on page 175.	Server C	From the **Reload Caches** heading: • Click **Reload** next to the **User List** field to load the User List. • Click **Reload** next to the **Global Address List** field to load the Global Address List.

Index

A

access mask 329, 330, 332
adding 329
changing 330
deleting 330
viewing 332
accessing 195, 270, 274
audit log 270
Caller Applications Editor 195
diagnostics results 274
port usage 270
account policies 28
login 28
activity log report 265
running 265
add network machine 114
field descriptions 114
add trusted server 106
field descriptions 106
adding 22, 42, 44, 87, 96, 98, 105, 113, 135, 146, 148, 156, 170, 172, 198, 218, 237, 319, 329, 361
access mask 329
Active Directory user 135
additional application server 98
additional sites 87
backup schedule 218
Class of Service 156
ELA list 172
first application server 96
holiday schedules 198
info mailbox 146
mailbox gateway 42
mailboxes 148
network server 113
new external host 42
Organizational Forms Libraries 22
postmaster mailbox 44
shadow mailbox 170
SNMP filter 237
static route 361
trusted certificate 319
trusted server 105
user 135, 148
additional sites 87
adding 87
addressing 152
remote users 152
administering 41, 100, 131, 176, 239, 306
ELA list 176
external SMTP hosts 41, 131
general options 306
load balancer 100
mail gateway 131
SNMP agent 239
administration history log 252, 253
field descriptions 253
viewing 252
administrator 31, 254
changing password 31
log field descriptions 254
advanced 122, 123, 208, 355, 357
configuring dial-in rules 123
configuring dial-out rules 122
installing software 208
miscellaneous 357
timeout 355
agent 239
administer SNMP 239
agent status 242
changing 242
viewing 242
alarm 227, 256, 332
levels 227
log field descriptions 256
overview 227
testing origination 332
viewing logs 256
alarms 228
alias 19
application 33, 58, 72, 73, 95, 348
backing up files 72
backing up server 72
restoring files 73
role 33, 58, 95
verifying status 348
application role 57
deployment scenarios 57
application server 96, 98, 266, 337, 434
adding 96, 98
diagnostics 337
logs 266
time zone 98

application servers 119
assigning 86
attendant number 86
assigning languages 88
site 88
attendant 86
assigning number 86
attended backup 213
audio prompt 183
audio prompts 199
uploading 199
audit log 270
accessing 270
Authentication file generation date 325
Auto Attendant 27
Avaya Authentication 325
AxC 58, 71, 103, 348, 356
address 58
changing address 71
testing connectivity 103
verifying status 348
viewing address 356

B

backing up 72, 213, 216
application files 72
application server 72
system files 213
System Platform 216
backup 58, 211, 218, 219
adding schedule 218
changing schedule 219
deleting schedule 219
backup error 434
backup Messaging system 393
configuration information 393
Backup page 217
field descriptions 217
backup screen 214
field descriptions 214
broadcast message 168
broadcast messages 158, 203
busy out voice equipment 311
field descriptions 311
busyout 310
voice channels 310

C

CA 327
cache statistics 351
monitoring 351
calculation 224
storage space 224
call drop 433
call records 270
viewing 270
Caller Applications 181–185, 187–189, 194, 195, 197–199
changing password 194
checklist 188
container 182, 189, 195
deploying 199
menus 184, 185, 189, 197
prompts 183
schedules 187, 198
system requirements 181
Caller Applications Editor 181, 194, 195
installing 194
logging in 195
capacity 95
CAS array 100
load balancer 100
caveats 390
certificate 323
application 323
server 323
Certificate Authority 327
certificate signing 315
certificates 322–324
adding server applications 323
copying 324
deleting 324
displaying 322
server/application 322
change password 151
changing 31, 39, 71, 99, 136, 183, 194, 219, 235, 237, 242, 330, 363
access mask 330
administrator password 31
agent status 242
AxC address 71
backup schedule 219
Caller Applications password 194
hostname 363
IP address 363
LDAP root password 39
role 99
SNMP filter 237
SNMP trap 235
storage server role 99
user properties 136

wav file format 183
checklist ...33, 37, 58, 74, 81, 188, 293, 295, 394, 402, 407, 413, 419, 424, 429, 439
application administration 58
caller applications 188
changing the server role 439
duplicated application server configuration 394, 402, 407
initial administration 33, 37, 58, 81
maintenance 293, 295
message store redundancy configuration 429
Messaging configuration 74
shared application server configuration 413, 419, 424
sites and topology administration 81
storage administration 37
Class of Service 155–158
adding 156
deleting 157
field descriptions 158
modifying 157
cluster 81, 95, 99, 102, 103, 130
configuring 99, 102, 130
field descriptions 103
time zone 95
CNAME 19
cofiguring 130
storage capacity 130
collect 269
system log files 269
configuration 225
restoring for System Platform 225
configuration information 393
backup Messaging system 393
primary Messaging system 393
configure 46
minimum service permissions 46
configuring ...43, 45, 47, 48, 52, 83, 99, 108, 109, 122, 123, 125, 130, 143, 153, 170, 233, 264, 266, 307, 354, 357, 359
advanced dial-in rules 123
advanced dial-out rules 122
cluster 99, 130
EWS 52
IMAP4 access 109
impersonation permissions 47, 48
logs 266
mail options 307
mailbox number length 43
Messaging parameters 108
miscellaneous information 357
network settings 359
postmaster mailbox number 45
privacy enforcement level for IMAP4 clients 109
remote updates 153
shadow mailbox 170
site properties 83
SNMP trap destinations 233
storage destination 52
system parameters 125
system policies 143
timeouts information 354
user activity log 264
core files 358
enabling 358
generation 358
creating 46, 183
.wav file 183
Messaging Service Account 46
current alarms 229
field descriptions 229

D

data backup 218
defining 85
dial rules 85
deleting .. 137, 149, 157, 168, 208, 219, 235, 237, 330, 361
access mask 330
backup schedule 219
broadcast message 168
Class of Service 157
mailboxes 149
network route 361
SNMP filter 237
SNMP trap 235
software packages 208
user 137, 149
deployment scenarios 57
diagnose voice equipment 313
field descriptions 313
diagnosing 312
voice equipment 312
diagnostics 244, 274, 313, 332–337
accessing results 274
alarm origination 332
application server 337
diagnose voice equipment field descriptions 313
IMAP4 connection 334
LDAP test connection 333
mail delivery 335
name server lookup 336
POP3 connection 334

SMTP connection 333
system logs 244
diagnostics (Application) 337
field descriptions 337
dial rules 85, 119, 122, 123
defining 85
field descriptions 119
Dial rules 133
disabling 328
services on the server 328
display voice equipment status 313
field descriptions 313
distribution list 158, 169, 170, 176
DNS record 19
document changes 15
document purpose 15
documentation 15, 16
administration 16
downloading files 318
duplicated application server 394, 402, 407

E

E.164 Dial Plan support 82
ELA 169, 172, 173, 176, 263
adding list 172
administering list 176
delivery failure log field descriptions 263
field descriptions 173
overview 169
emergency plan 373
application server 373
enabling 49, 67, 328, 358
basic authentication for Exchange 2007 49
basic authentication for Exchange 2010 49
core files generation 358
fax 67
services on the server 328
Enhanced-List Application (ELA) 169
Enhanced-List Membership 179
field descriptions 179
Enhanced-List Membership Report 180
field descriptions 180
ensure 203
voice quality 203
ensuring 203
teletypewriter users receive broadcast messages 203
EWS 52
Exchange 2007 support 47
Exchange 2010 support 48
Exchange server 20
Exchange Web Services 52
executing 339, 341, 344
Netstat 344
ping 339
traceroute 341
external hosts 37, 41, 131
administering SMTP 41, 131

F

failover behavior 378
failover experience 378
fax 66, 67, 124
enabling 67
types 124
field description 336
Name Server Lookup Results 336
field descriptions 29, 32, 42, 53, 61, 69, 89, 102, 103, 106, 107, 110, 114, 117–119, 121, 125, 138, 139, 143, 146, 158, 167, 171–173, 177, 179, 180, 196, 214, 221, 223, 229, 231–233, 240, 245, 253–256, 258–265, 267, 269, 275, 279–282, 284, 285, 287, 289, 291, 301–303, 305, 306, 308, 311, 313, 315, 317, 318, 325, 326, 328, 333–337, 350, 352, 356, 359, 360, 362, 364, 366, 369, 374
log configuration 267
add network machine 114
add trusted server 106
administration history log 253
Administration History Log 253
Administrator Accounts 32
administrator log 254
Administrator's Log 255
alarm log 256
Alarm Log Results 258
Alarm Summary 232
Audit History 302
Authentication File 326
AxC Address 356
Backup Logs 221
backup screen 214
busy out voice equipment 311
Certificate Alarms 231
Certificate Signing Request - Form 317
Class of Service 158
cluster 103
Collect System Log Files 269
configure user activity log 264
Core Files 359
create a new Enhanced-List page 173
current alarms 229

diagnose voice equipment 313
diagnostics (Application) 337
Dial Plan Handling Test 121
dial rules page 119
display configurations 362
display voice equipment status 313
Download Files 318
ELA delivery failure log 263
Enhanced-List Membership 179
Enhanced-List Membership Report 180
general options 306
info mailbox 146
information mailboxes 280
Internet messaging page 262
Internet Messaging Traffic 287
Internet Messaging:IMAP4 Connection Test 335
Internet Messaging:POP3 Connection Test 334
Internet Messaging:SMTP Connection Test 333
language packs 69
local users 279
locked out users 285
login account policy 29
login failures 284
Login Reports 291
mail delivery test 335
mail options 308
maintenance log 260
Maintenance Log Results 261
Manage Enhanced-Lists 172
Manage Networked Servers 114
Manage Trusted Servers 106
manage updates 364
Messaging Database Audits (Storage) 301
messaging measurements 289
mobile operators 167
network configuration 360
Network Snapshot 118
New Caller Application 196
new external host 42
Octel Aria 305
process status 369
process status results 369
release voice equipment 315
remote users 281
Report of Enhanced-Lists 177
Report of Network Servers 117
Report of Server Ranges 119
Report of Trusted Servers 107
Server/Application Certificates 325
sites 89
SNMP Agents screen 240
SNMP trap destinations 233
software management log 259
software version 374
Sort Enhanced-List 177
SSH Keys 328
static routes 362
status summary 366
storage destinations 53
syslog server 275
system logs 245
system mailboxes 171
System Operations 352
system parameters 125
system policies 143
system ports and access 110
telephony integration 61
Test Name Server Lookup 336
topology page 102
uninitialized mailboxes 282
user activity log 265
user management 138
user management properties 139
verify LDAP processes 303
View/Restore Data 223
voice channels 350
filter 237
SNMP 237
Filter 236
SNMP 236
filters 237
SNMP 237
filters screen 238
field description 238
Firewall 327
flexible storage 45
for replying to messages 133
forms 20
voice messaging 20
front-end/back-end 95

G

gateway 165, 166
mail 165, 166
general options 306
administering 306
field descriptions 306
generate 242
test trap 242
generate new SSH keys 328
global address list 175

loading 175
greetings 161

H

hardware requirements 391
holiday schedules 187, 198
adding 198

I

IMAP/SMTP 309
status 309
IMAP/SMTP status 309
verifying 309
IMAP/SMTPSetting 307
mail options 307
IMAP4 ..... 108, 109, 334
configuring access 109
configuring privacy enforcement level 109
testing connection 334
implementing 66
fax 66
implementing fax 66
important information 202
TTY 202
importing 304
Octel Aria data 304
improved multisite support 82
inbound fax 124
limitations 124
info mailbox 145, 146
adding 146
field descriptions 146
initial administration 33
checklist 33
install Certificate Using Internet Explorer 327
install Root Certificate 327
installing 24, 194, 206, 208
advanced software 208
Caller Applications Editor 194
software 206
voice message form 24
intended audience 15
Internet messaging 261, 262, 277, 286
field descriptions 262
traffic 277
viewing 261
viewing traffic 286

L

language 21, 58, 68
configuring 68
packs 58
voice messaging forms 21
language packs 67, 69
field descriptions 69
LDAP 39, 303, 333
changing root password 39
testing connection 333
verify processes field descriptions 303
verifying processes 303
library 20
organizational forms 20
license 392
requirements 392
License 27
management 27
license status 158
licensing 157, 158
basic 157
mainstream 157
limitations 124
inbound fax 124
load balancer 100
administering 100
CAS array 100
loading 175
global address list 175
user list 175
log 247
system 247
log out 35
logging in 33, 195
Messaging 33
to Caller Applications Editor 195
login account policy 28
login options 203
logon 328
logs 243, 252–254, 256, 259–267, 269, 270, 274, 275
accessing audit log 270
accessing ports usage 270
activity log report 265
administration history log 252
administration history log field descriptions 253
administrator log field descriptions 254
administrator's 243
alarm 243
alarm log 256
alarm log field descriptions 256
application server 266
call records 270
configuring 266

diagnostics results 274
ELA delivery failure log field descriptions 263
IMAP/SMTP Messaging 261
Internet messaging log field descriptions 262
Internet messaging logs 261
maintenance 243, 259
maintenance log field descriptions 260
software management 259
software management log field descriptions 259
storage server 252
syslog server 275
system log files 269
system log filter 267
user activity 243
user activity log field descriptions 265
user activity logs 264

M

mail 37, 42, 307, 335
configuring options 307
options 37, 42
testing delivery 335
mail gateway 131, 165, 166
changing 131
testing 166
mail options 308
field descriptions 308
mailbox 42, 145, 149–151
adding gateway 42
change password 151
info 145
reset password 150
unlock account 149
mailbox number length 43
configuring 43
maintenance checklist 293, 295
application server 293
storage server 295
maintenance log 260
field descriptions 260
Manage Enhanced-Lists 172
field descriptions 172
Manage Networked Servers 114
field descriptions 114
Manage Trusted Servers 106
field descriptions 106
manage updates 364
field descriptions 364
managing 178
enhanced-list administrators 178
enhanced-list members 178
mapping tables 134
measurements 153, 277
memory usage 376
message 133, 163, 164
retention 164
storage 163
message failure 436
message mirror 96
Message Mirror 381, 390
message recording 124
Messaging 108
configuring parameters 108
messaging measurements 289
field descriptions 289
Microsoft Outlook 20
migrating 84, 304
dial plan data 84
Octel Aria data 304
migration 304
Octel Aria 304
mobile operators 165–167
adding 165
field descriptions 167
testing gateways to 166
modifying 22, 23, 157
Class of Service 157
Organizational Forms Libraries 22, 23
monitoring 349, 351
cache statistics 351
voice channels in real time 349
Mutare 96, 392
server hardware specificationd 392
MWI 435

N

name server lookup 336
diagnostics 336
testing 336
netstat 344, 346
results 346
Netstat 344, 345
executing 344
field descriptions 345
network 19
network configuration 359, 360
field descriptions 360
network machine 37
network server 113
adding 113
network settings 359

configuring 359
Network Snapshot 118
field descriptions 118
New Caller Application 196
field descriptions 196
nightly maintenance 124
notification 162
notifications 228
Notify Me 133, 162

O

Octel Aria 304, 305
options for replying to 133
Organizational Forms Libraries 22, 23
adding 22
modifying 22, 23
Organizational Forms Library 21
outcalling 162
Outlook 20
overview 201
TTY 201

P

password 28, 158
aging 158
guidelines 28
patch installation 206
performance monitoring 376
performing 221, 301
restore 221
voice messaging database audit 301
ping 339, 340
field descriptions 339
results 340
Ping 339
executing 339
policies 28
login account 28
POP3 connection 334
diagnostics 334
testing 334
port 61, 95, 270
accessing usage 270
UDP range 61
port usage report 271
postmaster mailbox 44, 45
adding 44
configuring number 45
primary Messaging system 393
configuration information 393
privacy enforcement 108
privileged administrator login 30
adding 30
process status 369, 376
viewing results 369
properties 136
user 136
purpose of document 15

R

RBAC 329
redundancy 95
release voice equipment 315
field descriptions 315
releasing 314
voice channels 314
reload 352
Application server cache 352
reload caches 175
remote updates 134, 152, 153
configuring 153
running 153
remote users 151
report 271, 277
port usage 271
types 277
Report of Enhanced-Lists 177
field descriptions 177
Report of Network Servers 117
field descriptions 117
Report of Server Ranges 119
field descriptions 119
Report of Trusted Servers 107
field descriptions 107
reports 153, 277–280, 282, 283, 285, 286, 289
information mailboxes 279
local user 278
locked out users 285
login failures 283
remote update manually 153
remote user 280
system evaluation report 286
traffic measurement report 289
uninitialized mailboxes 282
Request Update 154
requirements 391, 392
hardware 391
server software 392
software 391
reset password 150

restore 58, 211, 221, 226
data 58
performing 221
viewing history 226
Restore page 225
field descriptions 225
restoring 73
application files 73
restoring System Platform configuration information 225
role-based access control 329
running 153, 265, 267, 289
activity log report 265
remote updates manually 153
system log filter 267
traffic measurement report 289
running audit 302

S

schedule backup 217–219
security 28
passwords 28
selecting 55
storage destination 55
sending logs 275
syslog server 275
server 20, 27, 59, 60, 95
Exchange 20
front-end/back-end 95
management 27
single server 95
SIP proxy 60
telephony 59, 60
server software requirements 392
Mutare 392
setting 202
TTY 202
shadow mailbox 170
adding 170
configuring 170
shared application server 413, 419, 424
shut down server 372
shutting down 373
application server 373
server 373
single site 381–385, 387, 388
SIP connections 60
SIP info messages 60
site 88
language choices 88
sites 81–83, 87, 89
adding additional sites 87
configuring properties 83
field descriptions 89
initial administration 82, 83
SMI 27
SMTP connection 333
diagnostics 333
testing 333
SNMP 233, 235–237, 239
adding filter 237
administering agent 239
changing filter 237
changing trap 235
configuring trap destinations 233
deleting filter 237
deleting trap 235
filter administration 236
SNMP Agents screen 240
field descriptions 240
SNMP trap destinations 233
field descriptions 233
SNMP traps 232
software 205, 206, 208, 259
deleting packages 208
installing 206
management log field descriptions 259
viewing installed 205
software requirement 391
Sort Enhanced-List 177
field descriptions 177
speech recognition 137
SSH 328
SSH keys 328
start Messaging 39, 377
static route 361
adding 361
static routes 360
status 40
storage role 40
stop Messaging 39, 377
storage 33, 37, 95, 163, 252
messages 163
role 33, 37, 95
server logs 252
storage capacity 130
offline call answering 130
storage destination 45, 52, 55
configure 52
select 55
storage destinations 37
storage space 224
support 17

contact ... 17
syslog server ... 275
field descriptions ... 275
sending logs ... 275
system ... 37–40, 45, 67, 95, 125, 170, 175, 194, 207, 213, 244, 245, 247, 267, 269, 277, 286, 377
backing up files ... 213
capacity ... 95
collect log files ... 269
configuring parameters ... 125
diagnostics logs ... 244
evaluation report ... 277
log results ... 247
logs ... 247
logs field descriptions ... 245
mailboxes ... 37, 45, 170
operations ... 175
parameters ... 67
policies ... 194
running log filter ... 267
start ... 39, 377
status ... 37
stop ... 39, 377
verifying clock ... 38
verifying installation ... 207
verifying status ... 40
viewing evaluation report ... 286
viewing logs ... 244
system log filter ... 268
field description ... 268
system mailboxes ... 171
field descriptions ... 171
System Management Interface ... 27
system parameters ... 125
field descriptions ... 125
system policies ... 143
configuring ... 143
field descriptions ... 143
system ports and access ... 108–110
field descriptions ... 110
system requirements ... 181
Caller Applications ... 181

T

TCP/IP ... 277, 288
snapshot ... 277
viewing snapshot ... 288
telephony ... 58–60
integration ... 58–60
telephony integration ... 61
field descriptions ... 61
telephony server ... 59, 60
integration ... 59, 60
telephony server integration ... 59, 60
teletypewriter ... 201
test trap ... 242
sending ... 242
testing ... 103, 332–336
alarm origination ... 332
AxC connectivity ... 103
IMAP4 connection ... 334
LDAP connection ... 333
mail delivery ... 335
name server lookup ... 336
POP3 connection ... 334
SMTP connection ... 333
Text to Speech ... 183
topology ... 81, 95, 96, 98, 102, 103
field descriptions ... 102
front-end/back-end ... 95
initial administration ... 95
single server ... 95
testing connectivity ... 103
traceroute ... 341, 343
results ... 343
Traceroute ... 341, 342
executing ... 341
field descriptions ... 342
traffic ... 19
network ... 19
traffic measurement report ... 289
running ... 289
traffic measurements ... 376
training courses ... 16
traps ... 232, 233, 235
SNMP ... 232, 233, 235
troubleshooting ... 433–437
backup error ... 434
call drop ... 434
fax ... 437
message failure ... 436
message undelivered ... 436
MWI ... 435
resetting G450 for DTMF ... 433
user recognition ... 435
trusted ... 105, 319
adding server ... 105
certificates ... 319
trusted certificate ... 322
field description ... 322
TTY ... 201, 203
login options ... 203

U

UDP port 61
unlock voice mailbox 149
update 134, 153
  configuring remote updates 153
  remote user list 134
uploading 199
  audio prompts 199
user 37, 133, 135–137, 148, 149, 264, 277
  activity logs 264
  adding 135, 148
  changing properties 136
  configure activity log field descriptions 264
  configuring activity log 264
  deleting 137, 149
  local 133
  remote 133
  reports 277
user activity log 265
  field descriptions 265
user list 175
  loading 175
user management ... 44, 133, 135, 137, 138, 146, 148, 149, 170
  field descriptions 138
user management properties 139
  field descriptions 139
User Preferences 162
  Notify Me 162
user recognition 434
utilities 300
  messaging database audit 300

V

validating 65, 74, 429
  message store redundancy configuration 429
  Messaging configuration 74
  telephony integration 65
verifying 38, 40, 207, 303, 309, 348
  application status 348
  AxC status 348
  IMAP/SMTP status 309
  LDAP processes 303
  system clock 38
  system installation 207
  system status 40
videos 17
view 254, 259
  administrator's log 254
  maintenance logs 259
viewing 29, 205, 220, 224, 229, 231, 232, 252, 256, 261, 263, 270, 271, 278–280, 282, 283, 285, 286, 288, 290, 332, 351, 356, 362, 366, 368, 369, 374
  access mask 332
  administration history log 252
  alarm logs 256
  alarm summary 232
  AxC address 356
  backup history 220
  backup logs 220
  cache statistics 351
  call records 270
  certificate alarms 231
  current alarms 229
  display configurations 362
  ELA delivery failure logs 263
  information mailboxes report 279
  installed software list 205
  Internet messaging logs 261
  Internet messaging traffic 286
  local user report 278
  locked out users report 285
  login account policy 29
  login failures report 283
  login reports 290
  port usage report 271
  process status 368
  process status results 369
  remote user report 280
  restore history 224
  software version 374
  status summary 366
  system evaluation report 286
  TCP/IP snapshot 288
  uninitialized mailboxes report 282
Voice Channel Monitor 350
voice channels 310, 314
  busyout 310
  releasing 314
voice equipment 312
  diagnosing 312
voice equipment diagnostics 310
voice message form 20, 24
voice messaging database audit 301
  performing 301
voice messaging form 21
  languages supported 21

W

warranty 18

wav file 183
Web Acesss Mask 331
overview 331