Administering Avaya Aura® Messaging

Release 7.1.0
Issue 9
April 2020

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named

User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

Contents

Chapter 1: Introduction

Purpose of this guide

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.

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

Change history

Issue	Date	Summary of changes
9	April 2020	• Updated the requirements for the postmaser mailbox in Adding the postmaster mailbox on page 70. • Added information about the new **Play record instructions to callers after a greeting** to System Parameters field descriptions on page 178. • Added information about the new **Reset the message waiting light on your desk phone** setting to User Management > Properties field descriptions on page 194. • Added MWI displays an incorrect status of user's voice messages on page 562.
8	October 2019	• Reorganized the "Organizational Forms Library" section. • Updated Supported languages on page 24. • Added Adding Organizational Forms Library to Exchange Server 2013 on page 27. • Updated Installing the voice message form on page 28. • Updated Adding a mail gateway on page 77. • Updated Language packs on page 115. • Updated System Parameters field descriptions on page 178. • Updated Mail Options field descriptions on page 393.

Table continues…

Issue	Date	Summary of changes
7	March 2019	• Indicated that the SIP entity type must be “Messaging” in Creating a SIP entity of a storage server on System Manager on page 98 and Creating a SIP entity of a storage server on System Manager on page 98. • Updated System Administration field descriptions on page 159. • Updated System Parameters field descriptions on page 178. • Updated information about the frequency at which traffic types collect data in Messaging Measurements field descriptions on page 366. • Added Remote messages traffic report on page 373. • Added Traffic snapshot report on page 377.
6	September 2018	• Added Usage of imported server identity certificates instead of the default identity certificate on page 401. • Added Managing Meltdown and Spectre vulnerabilities on page 417.
5	August 2018	• Indicated that Avaya Aura® Messaging supports TLS 1.2. • Updated Telephony Integration field descriptions on page 91. • Updated Changing Auto Attendant greetings on page 129. • Updated System Administration field descriptions on page 159. • Updated System Parameters field descriptions on page 178. • Updated Restoring data on page 294. • Updated Server Log Files field descriptions on page 345. • Updated Sending logs to an external syslog server on page 344. • Added Selecting a minimum supported TLS version required to access SMI on page 413. • Added Enabling or disabling Avaya Services access using ASG on page 414. • Updated Initial setup of a new mirrored Messaging system on page 501. • Updated Failback service to the primary system on page 511.
4	April 2018	• Removed support for Telnet. • Replaced Access Security Gateway (ASG) with Enhanced Security Gateway (EASG). • Removed support for FTP method in backup and restore. • Added procedure to create SIP entity for Avaya Aura® Messaging storage server. • Added procedure to add local host name entries for Avaya Aura® Messaging storage server.
3	January 2018	Added a procedure to restart the server.

Table continues…

Issue	Date	Summary of changes
2	December 2017	Removed support for the following servers: • Dell™ PowerEdge™ R610 • HP ProLiant DL360 G7 • CallPilot 1006r
1	January 2017	Added information about the following product enhancements: • Support for Windows 10 for Caller Applications Editor client, Fax desktop client, User preferences, and Messaging Web Access • Support for IPv6 format standard • Support for increasing system capacity to 30,000 or 40,000 local users, by restricting the following features and settings: - End-user use of external IMAP4 and POP3 clients - Messaging Web Access For 40,000 local users, restrict Notify Me, Reach Me, and Transfers. • Support for administrator configurable Message Waiting Indication with broadcast messages • Support for Admin SMI option for configuration of PIN password rules • Support for: - Class-of-Service settings for Rapid prompts - Class-of-Service settings for default message playback options

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

In the Domain Name System (DNS), you must create an A record, which contains the Messaging server host name. Using the information from the A record, DNS resolves the Messaging server host name to an IP address on the network. You can create a Canonical Name (CNAME) for the Messaging server in DNS. The CNAME record in DNS points to an A record and indicates that the domain name is an alias of another canonical domain name. To create an A record for an alias, use the following guidelines:

- Point the alias to the storage server if you have a front-end or back-end topology.
- Use `avayamsg` as the alias. For example, `avayamsg.example.com`. Use this alias name for the Messaging server.
- Ensure that your mail gateway:
  - Is configured to accept SMTP traffic from FQDN (Fully Qualified Domain Name) of the storage server.
  - Sends messages to the Internet domains.

- Is configured to grant IP access to the storage server.

Note:

For the proper functioning of Text-To-Speech, ensure that you have entered the FQDN of the server in the **DNS Domain** field.

Prepare for Exchange forms

Exchange Server administration overview

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

- Verify that your Exchange Server has the forms folders. If the folders are absent, you must create the form folder.
- Use Microsoft Office 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 Server:

- Exchange Server 2007
- Exchange Server 2010
- Exchange Server 2013

System folders are hidden folders for internal Exchange System Management. In large organizations with specialized administration roles, the Exchange Server 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 the Microsoft Exchange Server. You must assign permissions to individuals to publish to the 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 and gives the users an interface for performing actions such as:

- Playing

- Stopping
- Pausing voice messages
- Play on Phone
- Voice Reply
- Voice Forward
- 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 in:

- Preview pane: User previews a voice message.
- Separate window: User opens the voice message in a separate window.

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 following table lists the languages that Messaging supports for voice messaging forms.

Download the forms from `http://<Messaging storage server IP or FQDN>/download/<Voice messaging form file name>`

Language	File name
Arabic	AvayaVoiceMessage_ar-SA.fdm
Chinese-Peoples Republic of China	AvayaVoiceMessage_zh-CN.fdm
Chinese-Hong Kong	AvayaVoiceMessage_zh-HK.fdm
Dutch	AvayaVoiceMessage_nl-NL.fdm
English-US	AvayaVoiceMessage_en-US.fdm
English-US bilingual	AvayaVoiceMessage_en-US-BL **Note:** This bilingual pack also requires the French-Canadian language pack.
English-UK	AvayaVoiceMessage_en-UK.fdm
French	AvayaVoiceMessage_fr-FR.fdm
French-Canadian	AvayaVoiceMessage_fr-CA.fdm

Table continues…

Language	File name
French-Canadian bilingual	AvayaVoiceMessage_fr-CA-BL **Note:** This bilingual language pack also requires the English-US language pack.
German	AvayaVoiceMessage_de-DE.fdm
Hebrew	AvayaVoiceMessage_he-IL.fdm
Italian	AvayaVoiceMessage_it-IT.fdm
Japanese	AvayaVoiceMessage_ja-JP.fdm
Korean	AvayaVoiceMessage_ko-KR.fdm
Polish	AvayaVoiceMessage_pl-PL.fdm
Portuguese-Brazilian	AvayaVoiceMessage_pt-BR.fdm
Portuguese-European	AvayaVoiceMessage_pt-PT.fdm
Russian	AvayaVoiceMessage_ru-RU.fdm
Spanish	AvayaVoiceMessage_es-ES.fdm
Spanish-Latin American	AvayaVoiceMessage_es-XL.fdm
Swedish	AvayaVoiceMessage_sv-SE.fdm
Turkish	AvayaVoiceMessage_tr-TR.fdm

Organizational Forms Library

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

- Exchange Server 2007
- Exchange Server 2010
- Exchange Server 2013

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

Micorsoft Exchange Server 2007 or 2010

Adding Organizational Forms Library to Exchange Server 2007 or 2010

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

About this task

Use this procedure to modify and export the following:

- Exchange Server folder properties
- Export and import permissions
- Replica lists
- Enumerate items
- Gain access to mailboxes
- And other tasks

Do these tasks using 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. Run the `Exfolders.exe`.

   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

About this task

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

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.

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 then click **OK**.

   The MAPI editor opens Public Folder Management Console.
5. Expand **Public Root** > **NON_IPM_SUBTREE** > **EFORMS REGISTRY** and then select Organization Forms Library.
6. In the Property Name(s) column, click the **PR_URL_NAME** property.
7. Click **Property** > **Additional Properties** and then click **Add**.
8. In Property Tag Editor, click **Select Property Tag**.
9. In Property Selector, click **PR_EFORMS_LOCALE_ID** and then 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 and then click **OK**.

    For example, type `1033` for English.
15. Close MFCMAPI.

Microsoft Exchange Server 2013

Adding Organizational Forms Library to Exchange Server 2013

Procedure

1. Open Exchange Management Shell.

2. If you do not have a public folder mailbox, run the following command to create it:

```
New-Mailbox -PublicFolder -Name PFHierarchy
```

3. Run the following command to create a new folder for Organizational Forms Library:

```
New-PublicFolder -Path "\NON_IPM_SUBTREE\EFORMS REGISTRY" -Name "Organizational
Forms Library"
```

4. Run the following command to set a locale ID for the new folder:

```
Set-PublicFolder "\NON_IPM_SUBTREE\EFORMS REGISTRY\Organizational Forms Library" -
EformsLocaleID <LOCALE>
```

   In this command, `<LOCALE>` is the required locale ID. For example, to set the US English locale, run the following command:

```
Set-PublicFolder "\NON_IPM_SUBTREE\EFORMS REGISTRY\Organizational Forms Library" -
EformsLocaleID EN-US
```

   For more information about the Set-PublicFolder cmdlet, see Set-PublicFolder.

5. Run the following command to grant Owner permissions to a user that needs to create forms in Organizational Forms Library:

```
Add-PublicFolderClientPermission "\NON_IPM_SUBTREE\EFORMS REGISTRY\Organizational
forms library" -User <USER> -AccessRights Owner
```

   In this command, `<USER>` is the user principal name (UPN), domain\user, or alias of the user for whom you want to add Owner permissions.

Related links

Organizational Forms Library on page 25

Installing the voice message form

About this task

Use this procedure to install the voice message form on a computer that runs Microsoft Outlook.

Before you begin

Ensure that you:

- Have a system folder on Exchange Server that contains one Organizational Forms Library for each language in a multilingual deployment.
- Have an account with client permissions for administering Organizational Forms Library.
- Complete one of the following tasks:
  - Configure the avayamsg A or CNAME record in DNS.
  - Record the host name or the IP address of the Messaging server.

Procedure

1. Log in with the user account that you created in the `EFORMS REGISTRY` and that has client permissions.

2. In a web browser, navigate to `http://<Messaging storage server IP or FQDN>/download/<Voice messaging form file name>`, and save the form to a temporary location on your hard disk drive.

   For each language that you want to deploy, repeat Step 2 .

3. Open Microsoft Outlook and then do one of the following:
   - If you use Microsoft Outlook 2007, navigate to **Tools** > **Options** > **Other** > **Advanced Options...** > **Custom Forms**.
   - If you use Microsoft Outlook 2010 or newer, navigate to **File** > **Options** > **Advanced** > **Developers** > **Custom Forms**.
4. In the Options dialog box, click **Manage Forms**.
5. In the Forms Manager dialog box, click **Install**.
6. In the **Files of type** field, select **Form Message (*.fdm)**.
7. Select the voice message form file to install.
8. 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.

9. **(Optional)** 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, in Personal Forms, select **Avaya Voice Message**.
13. To copy the voice message form into your forms library, click **Copy**.

    If you are deploying multiple languages, repeat step 8 to 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.

    Note:

    If you use Microsoft Outlook 2010 and you do not see the form that you added, you must restart Microsoft Outlook.

Related links

DNS record on page 22
Supported languages on page 24

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
  - Internet Message Access Protocol 4 (IMAP)
  - Simple Mail Transfer Protocol (SMTP)
  - Users and Class of Service (CoS)
- The server administration interface to configure, maintain, and troubleshoot Messaging servers.

Note:

Some browsers might display SMI buttons differently than the buttons described in this document.

Administration passwords

Password complexity enhancement

The password policies apply to settings that use the Linux Pluggable Authentication Modules (PAM) for authentication on the virtual machine on which Messaging runs. PAM provides dynamic authorization for applications and services in a Linux system. This feature does not impact password authentication used by mailboxes.

Linux allows all-digit usernames, but Messaging previously required at least the first character of a username to be a letter. With the new policy, customers can have usernames with all-digits, all-letters, or any combination.

The password complexity options can be configured on the Login Account Policy page in Messaging System Management Interface.

The available username and password configuration options:

- All-digit usernames are allowed.
- Minimum password length.
- Required numbers of digits, lowercase letters, uppercase letters, and special characters.
- Number of old passwords that cannot be reused.
- Number of sequentially repeated characters allowed.
- Number of characters in the new password that must differ from the old password.
- Password must contain at least one uppercase character, a lower case character, a special symbol, and a number.
- Check against dictionary words.

Login Account Policy

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

Do not use the Login Account Policy webpage to administer logins whose credentials are not maintained on the local server. For login credentials that are not maintained on the local server, perform the administration of logins through root login using standard Linux commands.

Note:

Use the Login Account Policy webpage 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 webpage.

Login Account Policy field descriptions

Name	Description
Password Complexity Requirements: This section allows you to administer various password complexity options. Unless otherwise note, a value of 0 indicates that a requirement does not apply to a password.	
Minimum password length (minlen)	The minimum acceptable size for the password.
Minimum number of lowercase letters in a password (lcredit)	The minimum acceptable number of lowercase letters in the password.
Minimum number of uppercase letters in a password (ucredit)	The minimum acceptable number of uppercase letters in the password.
Minimum number of digits in password (dcredit)	The minimum acceptable number of digits in the password.
Minimum number of special characters in password (ocredit)	The minimum acceptable number of special characters in the password.
Number of previously used passwords to check for uniqueness (remember)	The number of previously used passwords that cannot be used as a new password.
Number of characters in the new password that must be different from old password (difok)	The minimum acceptable number of character changes in the new password that differentiate it from the old password.
Minimum number of character classes (minclass)	The minimum number of required classes of characters for the new password. The classes are digits, lowercase and uppercase letters, and special symbols.
Maximum number of consecutive repeating characters from the same class (maxclassrepeat)	The maximum number of the same consecutive characters of the same class in the password.
Maximum number of consecutive repeating characters in passwords (maxrepeat)	The maximum number of the same consecutive characters in the password.
Login Inactivity Timeout: This section allows you to administer how long idle sessions stay active. SMI is the System Management Interface, CLI is the command line interface. Both idle session timeout fields are in seconds.	
Maximum time an idle SMI session remains active (60 is the minimum)	The maximum time, in seconds, that an idle SMI session remains active. The minimum time that you can administer is 60 seconds, which indicates that the SMI session remains active for 60 seconds when there is no activity.

Table continues…

Name	Description
Maximum time an idle CLI session remains active (0 means disabled)	The maximum time, in seconds, that an idle CLI session remains active. If you set the value to 0, the maximum time limit for an idle CLI session to remain active is disabled. The CLI session remains active even when there is no activity.
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.
Login Limits: This section allows you to modify the login limits policy.	
Maximum number of simultaneous logins for a user	The maximum number of simultaneous logins for a user. If you set this value to 0, the system allows any number of simultaneous logins for the user.
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.
Make the faillock parameters apply to root as well	Specifies whether the root account can become locked.
Lock out account after the following number of unsuccessful attempts (DENY)	The values range from 1 through 9.
The failures must occur within this many seconds for the account to be locked (fail_interval)	The length of the interval during which the consecutive authentication failures must happen for the account to become locked.
Automatically unlock a locked account after the following number of seconds (UNLOCK_TIME)	The values range from 1 through 99999. If you set the value to 0, the locked account will *not* be unlocked automatically.

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 provides the highest level of access with the maximum permissions. A user with the privileged

administrator login can gain access to all the System management Interface pages and Command Line Interface.

Procedure

1. Log in to the Messaging System Management Interface.
2. In the **Administration** menu, click **Server (Maintenance)** > **Security** > **Administrator Accounts**.
3. In the **Select Action** area, select **Add Login**.
4. Select **Business Partner Login (dadmin)**.

   This login provides the highest level of access with the maximum permissions to a user. A user can gain access to all the SMI pages and CLI. You can add this login only once.
5. Click **Submit**.

   The system displays the Administrator Accounts -- Add Login: Privileged Administrator webpage.
6. Enter information in the following fields:
   - **Date after which account is disabled-blank to ignore (YYYY-MM-DD)**: Clear this field
   - **Enter password or key**
   - **Re-enter password or key**
7. Click **Submit**.
8. Click **Continue** to go back to the Administrator Accounts webpage.

Changing an administrator password

About this task

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

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

Procedure

1. Log in to Messaging with the privileged administrator login and password.

   If the privileged administrator login is nonexistent, 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. Type the new password in the **Enter password or key** field.

Some browsers automatically populate web-based forms with passwords. If **Enter password or key** contains a value, clear the field and enter the password. To prevent Messaging from automatically populating the passwords, turn off the option to remember the password in your browser.

6. Type the password again in the **Re-enter password or key** field.
7. Click **Submit**.

   The system changes the login password.

   If you do not enter a new password in Steps 5 and 6, your browser displays the following error after you click **Save**:

   ```
   You must enter a password.
   ```

Administrator Accounts field descriptions

Name	Description
Select Action	
Add Login	Select this option and select the type of login to add. The options are: • **Privileged Administrator**: Provides the highest level of access with the maximum permissions. A user can gain access to all the SMI pages and CLI. • **Unprivileged Administrator**: Provides restricted access. A user can gain access to the SMI pages that are for querying the Messaging status and backing up data and CLI. • **Web Access Only**: Provides access only to the SMI pages. A user can administer the SMI pages that the user can gain access to in the **Web Access Mask** settings of the profile of the user. • **CDR Access Only**: Not applicable. • **Business Partner Login (dadmin)**: Provides the highest level of access with the maximum permissions to a user and is similar to **Privileged Administrator**. A user can gain access to all the SMI pages and CLI. You can add this login only once. • **Business Partner Craft Login**: Provides the highest level of access with the maximum permissions and is similar to **Business Partner Login (dadmin)**. A user can gain access to all the SMI pages and CLI. With this login, the user can

Table continues…

Name	Description
	suppress alarms from the server when logging in to SMI. • **Custom Login**: Provides customized access. You can select the level of access to the user.
Change Login	The option to change a login.
Remove Login	The option to remove a login.
Lock/Unlock Login	The option to lock or unlock a login.
Add Group	The option to add a group.
Remove Group	The option to remove a group.

Checklist for administrators

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

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

Also, you must add all application servers and storage servers as network elements in System Manager. For more information, see *Administering Avaya Aura® System Manager*.

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:

No.	Task	Chapter number	Administrator type	Location		✔
				Single-server systems	Front-end / Back-end systems	
1	Prepare the network	Chapter 2	Network administrator	—	—	

Table continues…

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

Table continues…

Options	Description
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`. **Note:** Laptop setup for access via services port must be `192.11.13.5, 255.255.255.252`, and gateway of `192.11.13.6`.

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 the root certificate or the certificate chain for the 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**.

   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.

Accessing System Management Interface using IPv6

Before you begin

You must enable and configure IPv6 on the server.

With IPv6 enabled and configured IPv6, you can access the Messaging System Management Interface using both IPv6 and IPv4.

Procedure

Do the following:

- To access System Management Interface using IPv6: In your browser, type the following URL: `https://[<Messaging server IP>]` where <Messaging server IP> is the IPv6 address of the Messaging server.
- To access System Management Interface using IPv4: In your browser, type the following URL: `https://<Messaging server IP>` where <Messaging server IP> is the IPv4 address of the Messaging server.

Chapter 4: Initial administration of the storage role

Initial administration checklist for the storage role

Use the following checklist to set up a storage role on a server for the first time. In large organizations with specialized administration roles, the Messaging administrator usually performs these tasks.

No.	SMI page	Task	✔
1	License Status	License status on page 41.	
2	Server Date/Time	Verifying the system clock on page 41.	
3	Server Role / AxC Address	Administering the server role and AxC IP address on page 42.	
4	Telephony Domains	Adding telephony domains on page 48.	
5	Sites	Setting site properties for the first time on page 50.	
6	Topology	Adding the first application server on page 51.	
7	Topology	Activating sites on page 52.	
8	Networked Servers	Setting the length of mailbox numbers on page 69.	
9	System Administration	Configuring IMAP4 access on page 69.	
10	User Management	Adding the postmaster mailbox on page 70.	
11	System Mailboxes	Configuring the postmaster mailbox number on page 71.	
12	User Management	Creating a shadow mailbox on page 72.	
13	System Mailboxes	Configuring a shadow mailbox on page 73.	
14	User Management	Adding the broadcast mailbox on page 73.	
15	System Mailboxes	Configuring the broadcast mailbox number on page 74.	
16	External Hosts	Administering the external SMTP host on page 76.	
17	Mail Options	Adding a mailbox gateway on page 77.	
18	Change LDAP Password (Storage)	Changing the LDAP root password on page 78.	

Table continues…

No.	SMI page	Task	✔
19	Storage Destinations	Configuring a storage destination on page 79. Perform this task only if you use Exchange Server as a storage server.	
20	User Management	Selecting a storage destination on page 102. Perform this task only if you use Exchange Server as a storage server.	
21	System status	Verifying the status of the storage role on page 103.	

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**.

Verifying the system clock

About this task

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 NTP server to maintain accurate system time.

Before you begin

Check the system status to ensure that Messaging is running.

Procedure

On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Server Date/Time**.

The system displays the current date, time, and timezone.

Note:

If you change the system time, you must restart Messaging for the changes to take effect.

Next steps

Administer the server role.

Related links

Stopping Messaging on page 460
Starting Messaging on page 460
Administering the server role and AxC IP address on page 42
Initial administration checklist for the storage role on page 40

Administering the server role and AxC IP address

Messaging servers are set up for a single-server topology by default. Skip this procedure if you have a single-server topology.

About this task

Use this procedure to administer the server role and AxC IP address for the first time or to change the server role and IP address later.

AxC connects the storage and application roles. In a single-server topology, these roles are on the same server, and you can use the default settings. If your topology has multiple servers:

- Change the default AxC IP address on each dedicated application server.
- Secure communications between Web services and AxC.

If your deployment includes more than one server in the application role, change the AxC IP address only for the first server in the site. You can administer the servers for other application roles by backing up the first application role and then restoring the data on to the other application servers. For information about the procedures that you must perform manually on the server and the procedures that Messaging automatically performs through the backup and restore process, see *Initial administration checklist for application roles*.

Before you begin

- Administer the storage role.
- If you are administering the first dedicated application server or an application role in a single server, configure languages.
- Ensure that, on the AxC server, your server is added in the Messaging topology as an application server.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings** > **Server Role / AxC Address**.
2. In the **Server Roles** section, from the **Roles for this server** drop-down list, select the role of the server.
3. In the **AxC IP address** field, enter the IPv4 or IPv6 address of the storage server. You can specify the IPv6 address in this field, if IPv6 is enabled on the local server.

   By default, the Messaging system populates this field with the IP address of the local host. Ensure that the IP address that you enter belongs to an operational AxC server.
4. **(Optional)** To secure communications between Web services and AxC, in the **AxC Web Services Security** section, select **https://**.

   The default transport protocol is **http://**.
5. Click **Apply**.

   Messaging displays a confirmation message.
6. Click **OK**.
7. Restart Messaging or restart the server according to the displayed instructions.

Next steps

- Validate the Messaging configuration.
- If sites in the topology have only one application server, add telephony domains, and define the site and topology.
- If sites in the topology have multiple application servers, ensure that the configuration of the servers in the cluster is identical.

Related links

Adding telephony domains on page 48
Configuring languages on page 115
Adding the first application server on page 51
Backing up Messaging data on page 287
Restoring application files on page 288
Initial administration checklist for application roles on page 105
Initial administration checklist for the storage role on page 40
Initial administration checklist for sites and topology on page 120
Server Role / AxC Address field descriptions on page 44

Messaging configuration checklist on page 147

Server Role / AxC Address field descriptions

Name	Description
Server Roles	

Table continues…

Name	Description
Roles for this server	The option to select the role of a server. **Storage only** When you select this role, Messaging: • Disables the **AxC IP address** field and displays the 127.0.0.1 default IP address for the storage role in the field. • Disables the **Distributed Cache (ADCS)** fields and displays the default values in the fields. • Deletes all application roles associated with the server when you restart Messaging. When you select a storage-only role for the server, SMI does not display the following pages, which are specific to the application role: • Server Information: Voice Channels (Application), and Cache Statistics (Application) • Server Settings (Application): Dial Rules, Cluster, System Parameters, Languages, and Log Configuration • Advanced (Application): System Operations, Timeouts, Miscellaneous, and Core Files. • Logs: Call Records, Audit/Ports Usage, Diagnostics Results (Application) • Diagnostics: Diagnostics (Application), Diagnostics (ADCS) • Telephony Diagnostics (Application): Busy, Diagnose, Display, and Release **Application only** When you select this role, you must enter an IP address in the **AxC IP address** field. If you retain the 127.0.0.1 default IP address, which is the storage server IP address, or enter the local IP address of the server, Messaging displays a warning that you cannot

Table continues…

Name	Description
	enter the default IP address or the local IP address to administer the server for an application-only role. When you select an application-only role for the server, SMI does not display the following pages specific to the storage role: • Messaging System (Storage): User Management, Class of Service, Sites, Topology, Storage Destinations, System Policies, Enhanced List Management, System Mailboxes, System Administration, User Activity Log Configuration • Reports (Storage): Users, Info Mailboxes, Remote users, Uninitialized Mailboxes, Login Failures, Locked Out users, Sites, Dormant Mailboxes, Full Mailboxes • Server Information: Outbound Fax (Storage) • Server Settings (Storage): External Hosts, Trusted Servers, Networked Servers, Request Remote Update • IMAP/SMTP Settings (Storage): General Options, Mail Options, IMAP/SMTP Status • Telephony Settings: Telephony Domains • Utilities: Messaging DB Audits (Storage), LDAP Status/Restart (Storage), Change LDAP Password (Storage), CallPilot Migration, Octel Aria Migration • Logs: IMAP/SMTP Messaging, ELA Delivery Failures, User Activity • Server Reports: IMAP Traffic (Storage), SMTP Log Summary

Table continues…

Name	Description
	(Storage), Measurements (Storage) • Diagnostics: Alarm Origination, Network Connection, SMTP Connection, POP3 Connection, IMAP4 Connection, Mail Delivery, Diagnostics (Storage) **Storage and Application**: When you select this role, Messaging displays the 127.0.0.1 IP address in the **AxC IP address** field. You can change the IP address. The IP address in the **AxC IP address** field must be the 127.0.0.1 default IP address or the local IP address of the server.
AxC Address	
AxC IP address	The IP address of the storage server. The IP address must be the default address, which is 127.0.0.1 or the local IP address of the server.
AxC Web Services Security	
For web services communication with the AxC, use	The option to use a secure connection for web services communications with AxC. **https://** is the communications protocol for secure communications.
Distributed Cache (ADCS)	
Disk usage quota	The option to allocate a disk usage quota to ADCS. The default storage quota allocated to ADCS is: • 25 GB for the storage-only and storage and application roles. • 80 GB for the application-only role. The value that you enter must include the units of measure. For example, 80 G, 200 M, or 900 K. **Note:** This setting is an advanced setting. Consult your account representative before you enter data in this field.

Table continues…

Name	Description
Delete cached voice messages from the cache after	The option to administer the period after which Messaging automatically deletes the voice messages in the cache. The default period is 72 hours. You must set the **Delete cached voice messages from the cache after** to 1 day in System Management Interface.
Cache storage usage	A read-only field that displays the allocated storage quota used and the percentage.

Adding telephony domains

Before you begin

- Gather information about the parameters required to add telephony domains.

Procedure

1. On the **Administration** menu, click **Messaging** > **Telephony Settings** > **Telephony Domains**.
2. Enter the appropriate information in the fields.
3. Click **Save**.

Next steps

Administer the site properties.

Integrate the telephony domains with the application server.

Related links

Adding the first application server on page 51
Setting the site properties for the first time on page 50
Integrating with the telephony server on page 134
Integration requirements on page 133
Telephony Domains field descriptions on page 48

Telephony Domains field descriptions

Administer the telephony domain parameters that Messaging uses.

Far-end Domains

Name	Description
Far-end Domains	The number of far-end SIP domains. SMI displays the number of rows that are equal to the number of far-end SIP domains that you select from the drop-down list. You can add a maximum of 500 SIP domains.
Delete	The check box to delete a far-end domain row. Select the check box for the far-end domain row to delete.
Telephony Profile Name	The name for the telephony profile that represents a gateway ID and SIP domain of the application server. The name can contain alphanumeric characters along with a dash (-), underscore (_), and period (.).
Gateway ID	The ID of the far-end connection gateway.
Messaging SIP Domain	The name of the Messaging SIP domain.
Far-end SIP Domain	The name of the far-end connection SIP domain.

Far-end Connections

Name	Description
Far-end Connections	The number of connections to the far-end SIP proxy servers. SMI displays the number of rows that are equal to the number of far-end SIP domains that you select from the drop-down list. You can add a maximum of 25 far-end connections.
Delete	The check box to delete a far-end connection row. Select the check box for the far-end connection row to delete.
Gateway ID	The ID of the far-end connection gateway.
IP	The IP address of the far-end connection.
Transport	The transport method that the telephony server uses for SIP signaling. The transport method of the application server and the telephony server must match. The types of transport methods are: • **TCP**: Not encrypted. Use port 5060. This is the default value. • **TLS**: Encrypted. Use port 5061.

Table continues…

Name	Description
Port	The port number of the far-end connection. The default value is *5060*.
Monitor Interval	The option to administer monitoring of a far-end connection in minutes. The default value is **0** minutes. If you set the value to **0**, Messaging does not monitor the far-end connection.

Telephony Topology Reports

Name	Description
All	Displays all the reports of the far-end domains and connection.
Telephony Topology By Application Server	Displays a list of far-end domains that is filtered by the application server. Details include: • **Application Server (ID)** • **Site Name (ID)** • **Telephony Profile Name**
Telephony Topology By Telephony Profile Name	Displays a list of the profile names of the far-end domains.
Telephony Topology By Site	Displays a list of far-end domains that is filtered by the site. Details include: • **Site Name (ID)** • **Telephony Profile Name** • **Application Server (ID)**
None	No reports displayed.

Setting the 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 correctly. 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. Change the name of this site, and enter information about the primary messaging mailbox of your organization.

Perform this task on the storage server or the single server.

Before you begin

Add at least one telephony profile on the Telephony Domains page.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Sites**.
2. Complete the fields in the **Main Properties**, **Site External (Public Network) Dial Plan**, **Site Internal Dial Plan** areas.
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.

Next steps

- Add an application server to the topology.
- Add more sites to your network.

Related links

Adding telephony domains on page 48
Adding the first application server on page 51
Adding additional sites on page 126
Sites field descriptions on page 53

Adding the first application server

About this task

Perform this procedure on the storage 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.

Before you begin

- Configure the storage server and application servers.
- Create a site.
- Ensure that all application servers that you want 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 IPv4 or IPv6 address of the first application server. You can specify the IPv6 address in this field, if IPv6 is enabled on the storage server.
   b. In the **Add the server with** field, select **No active site configuration**.
   c. Click **Add**.

   Note:

   After you add a new application server, restart Messaging on the new application server.

Next steps

- Activate the sites in the topology.
- Add the application servers to the topology if your site has multiple application servers.

Related links

Administering the server role and AxC IP address on page 42
Setting the site properties for the first time on page 50
Activating sites on page 52
Adding additional application servers on page 132
Overview for administering sites on page 122

Activating sites

About this task

Perform this task to activate the sites after administering application servers to the sites.

Before you begin

- Administer the site properties.
- Add application servers to the sites.

Procedure

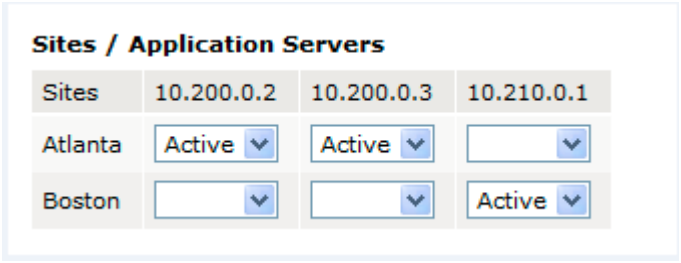
1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**.
2. In the **Sites / Application Servers** area, click **Active** from the drop-down list next to the site that the application server supports.
3. Click **Update**.

   Messaging displays a confirmation message.

4. Click **OK**.
5. Restart Messaging.

Example

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



Next steps

Administer the length of the mailbox numbers in your network.

Related links

[Setting the site properties for the first time](#) on page 50
[Adding the first application server](#) on page 51
[Adding additional application servers](#) on page 132
[Stopping Messaging](#) on page 460
[Starting Messaging](#) on page 460
[Setting the length of the mailbox number](#) on page 69

Sites field descriptions

Name	Description
Site	The drop-down list that displays all your Messaging sites.

Main Properties

Name	Description
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.

Table continues…

Name	Description
Telephony Profile Name	The profile name of the far-end SIP domain. You can add far-end SIP domains on the Telephony Domains page in the Telephony Settings section. • If far-end SIP domains are not configured, this drop-down list contains the **1** default value. • If far-end SIP domains are configured, this drop-down list contains a list of the SIP domains. **Note:** Ensure that you add at least one telephony domain before you create a new site or change a site. If the list of profile names does not match the list of far-end SIP domains on the Telephony Domains page, and there is no far-end SIP domain for a profile name, the far-end SIP domain might be deleted or the site might have been created before adding the far-end SIP domain.
Internal Messaging access number	The short number that Messaging expects to receive from the telephony server. The internal telephone number is called the internal pilot number. 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. **Note:** Messaging also allows non-unique **Internal Messaging access numbers** across sites. However the warning message: **Warning:** "You have entered duplicate numbers for your pilot number (Internal Messaging Access number) which could cause disambiguation issues if you are using short style extension numbers or do not have site identifiers for your sites. Proceed with caution." is displayed in this case.

Table continues…

Name	Description
External Messaging access number	The number that Messaging uses in notifications and in the General webpage in User Preferences to inform the user how to reach the Messaging system from outside. In Messaging, the call data of a call to the external number is identical to the call data of the internal number. The external telephone number is called the external pilot number. For example, a text notification sent to the mobile phone has a number for Messaging# . This number is identical to the number on User Preferences page, in Messaging Access Number section, in the **External** field.
Site Default Language	The drop-down list that displays the languages installed on the application server or the servers associated with a site. Use this option to select the default or the first language for a site. The default base language is English-US. The system uses the selected language to determine the language of the prompt that Messaging plays to callers who leave messages for all mailboxes within the site.
Additional Language	The drop-down list that displays the languages installed on the application server or the servers that are associated with a site. Use the options to select two additional languages for a site. When you select another language, callers leaving messages for all mailboxes on this site receive a multilingual prompt.

Site External (Public Network) Dial Plan

Messaging users can gain access to their mailbox by dialing the external Messaging access number, which is defined in the **External Messaging access number** field, from their mobile phones too. For this feature to work, the mobile phone number entered in the **Mobile Phone or Pager** field in the General tab of User Preferences must be identical to the number displayed in the caller ID of the telephone. When you define the dial plan, ensure that you consider the effects of the dial plan rules on the incoming number when a user calls from a mobile phone.

Name	Description
Country code	The country code of the dialed phone number. The country code must match the code where the site is located. For example, the country code for North American Numbering Plan countries (e.g. United States, Canada) is 1. For United Kingdom the country code is 44.

Table continues…

Name	Description
International prefix	The digits preceding the country code of the dialed telephone number. For example, if callers in the United States or Canada want to call the Dunedin City Council, they would dial 011 64 3 477 4000. (The International prefix for North American Numbering Plan countries is 011, the country code for New Zealand is 64, the area code for Dunedin is 3, and the local number for the Dunedin City Council is 477 4000). If callers in Japan want to call the same number, they would dial 010 64 3 477 4000 (010 is the international prefix for Japan). If callers in Australia want to call the same number, they would dial 0011 64 3 477 4000 (0011 is the international prefix for Australia). If callers in Italy want to call this number, they would dial 00 64 3 477 4000 (00 is the international prefix for Australia).
National prefix	The digits preceding the area code of the dialed phone number. In many countries, such as Australia, Germany and the United Kingdom, the national prefix is 0. In the North American Numbering Plan countries the national prefix is 1. For example, calling inter-area (within Australia): if callers in the Western Australia (area code is 8) want to call the Australian Area/State of Queensland (with the local number of xxxx xxxx and the area code of 7) they would dial 0 7 xxxx xxxx.
International dialing (to this country)	The option to prefix to the national code for international calls. The options are: • **Do not prepend National Prefix**. • **Prepend National Prefix**. For example, if callers in the United States want to call Rome, they would dial 011 39 0 6 xxxx xxxx. (The International prefix for North American Numbering Plan countries is 011, the country code for Italy is 39, the National prefix for Italy is 0, the area code for Rome is 6, and the local number for Rome xxxx xxxx). Alternatively, using a GSM cell phone, callers would simply dial +39 0 6 xxxx xxxx from the United States.

Table continues…

Name	Description
National destination code	The starting sequence of digits that the telephony server processes as local numbers, except for the number defined for the telephony server. For example, If you have more than one local area code in a given city (e.g. in the United States, New Jersey has 201, 551, 609, 732, 848, 856, 862, 908, 973 area codes) you can specify these codes in the Local Calls section.
Dialing within national destination	The option that Messaging uses for dialing a destination within the national code. 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 number of digits required to call a number within the originating area code or a local call. For example, New Jersey has ten digit dialing within area code. **Subscriber number length** for New Jersey is 7. Your call will be recognized as a local call if you dial (national destination code + seven digit number).
Outside line prefix	The digits required to access an outside line.

Site Internal Dial Plan

Name	Description
Short extension length	The extension length for the users on this site. If the **Short extension length** of the **Internal Dial Plan** equals the **Subscriber number length (within this site's national destination code)** of the **External Dial Plan** then it is necessary to use the Internal Calls section to determine internal subscriber numbers (extensions) that belong to the current site. Otherwise all numbers which length equals **Subscriber number length (or Short extension length)** will be considered as Local for this Site and will be handled by the **External Dial Plan**.

Table continues…

Name	Description
Short mailbox length	The mailbox number length for the users on this site. The short mailbox length is the length of the mailbox number without the country code and the site prefix. This length describes the internal extension length. For example, for a 5-digit based site with the long mailbox number 14085671234, the: • Site prefix is 40856. • Site country code is 1. • Site mailbox length is 4. • Short mailbox number is 71234.
Extension style for telephony integration	The extension style for telephony integration that defines the format that Messaging expects from an incoming call. The system uses this value to set MWI on or off. The options are: • **Short**: Messaging checks the values in **Internal Messaging access number** and **External Messaging Access Number** to identify the number in the incoming call. • **E.164**: Messaging processes the number in the incoming call as an E.164–format number. • **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.

Table continues…

Name	Description
Site prefix	The digits before the short extension digits. For example, for a 5-digit based site with the long mailbox number 14085671234: • The site prefix is 40856. • The site country code 1. • The site mailbox length 5. • The short mailbox number is 71234. Messaging uses the combined values of **Site prefix** and **Country code** as a site identifier. The site identifier is based on the values in: • **Extension style for telephony integration** • **Country code** • **Site prefix** Messaging checks the extension number of the calling user or the called user. If the site identifier matches the starting digits of the extension, Messaging considers the site as the home site to identify the user. With Messaging checking the site identifier as one of the parameters to match the extension and identify the site, sites are not bound by the maximum hunt group limit.
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 the users in this site: • **local** • **national** • **global** **Universal addressing** describes the acceptable recipient mailbox format which the TUI recognizes during login or using the **Send Message** feature to send a voice message from one mailbox directly to another mailbox without ringing the phone of the recipient or transfer to another mailbox.

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.

Name	Description
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. Separate the numbers with a semicolon (;). For example, 800; 844; 855; 866; 877; 888 are the toll-free codes for North American Numbering Plan countries.
Premium Number codes	The code used for dialing premium number calls. Even if you have highest dialout privileges, Messaging does not support calls to the premium numbers. Enter the national destination codes only. Do not include the national prefix. Separate the numbers with a semicolon (;). For example, 900 is the premium code for North American Numbering Plan countries.

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.

Name	Description
This site contains users whose Class of Service dial-out privilege allows only local calls	The option to indicate that the dial-out privilege of some users on this site is only to 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	The option to indicate that all local calls are not charged at local-call rates. 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 starting digits only. Do not include the national destination code. Separate multiple ranges with semicolons (;). 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.

Table continues…

Name	Description
Some national calls (calls outside the national destination code's area) are charged as local calls	The option to indicate that some calls to national numbers and to numbers outside the national destination are charged at local-call rates. 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 starting digits only. Do not include the national prefix. Separate multiple ranges with semicolons (;). 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.

Internal Calls

Call classification information for outbound calls, which is required to determine whether the call must be handled by Internal or External Dial Plan.

Name	Description
Internal Short extension length matches External subscriber number length	The option to indicate that the **Short extension length** of the **Site internal Dial Plan** matches the **Subscriber number length (within this site's national destination code)** of the **Site External (Public Network) Dial Plan** . For example, consider the UK_Derby site with the following configuration: • **Subscriber number length (within this site's national destination code)**: 6 • **Short extension length**: 6 • **Short mailbox length**: 6 In this case, the **short extension length** = **Subscriber number length (within this site's national destination code)** = 6.

Table continues…

Name	Description
Internal subscriber numbers	The user number that the system considers as internal. Define internal subscriber numbers using the regular expression syntax. For more information, refer to *Regular expressions for phone number translation rules*. Separate multiple regular expressions with semicolons (;). To enable this field, select the **Internal Short extension length matches External subscriber number length** checkbox. **Note:** Regular expressions do not always determine the exact length of numbers. Only numbers whose length equals Short extension length of the Site Internal Dial Plan can be considered as Internal.

Dial Plan Handling Test

The test to verify categories of phone numbers based on Internal and External Dial Plans. This test can be only performed for the site which:

- Has no unsaved Dial Plan changes.
- Is in the active state on atleast one application server with a site-based dial plan handling style.

Name	Description
Phone number	The phone number for verification of the **Site Internal Dial Plan** and the **Site External (Public Network) Dial Plan** configurations. You can verify the correctness of the **Site Internal Dial Plan** and the **Site External (Public Network) Dial Plan** handling by entering the phone number and clicking **Test**.
Phone number category	The phone number category of the **Phone number** that is based on **Site Internal Dial Plan** and **Site External (Public Network Dial Plan)**. You can get the phone number category by entering the phone number into the **Phone number** field, and clicking the **Test** button.

P-Asserted Identity

Name	Description
Customize identity information	The option to customize the identity information in the P-AI header. This check box is not selected by default. • Select the check box to customize the P-AI header and enter your values in **Name** and **Number**. • Clear the check box to overwrite the customized values with the default values, which are the values of **Site Name** and **Site Pilot Number**. When you clear the check box, the **Name** and **Number** fields become inactive. The caller ID that a called user receives might be different than what you administer in the P-AI headers. Earlier Messaging releases did not support custom identity information, so the values of the P-AI headers might be determined by other components in the network. Depending on the feature that starts the outbound call and whether the incoming caller ID is available, the following table lists how Messaging determines the P-AI header value. • Caller: Sets the P-AI header value based on the incoming call. • Subscriber: Sets the header value based on the value administered for the extension of the user. • Site: Sets the header value based on the value administered for a site.
Name	The name that you want to enter in the identity information of the P-AI header. The maximum length of this field is 100 characters. If you enter more than 100 characters or leave this field blank, SMI displays a warning when you save the updates to the Sites page.
Number	The number that you want to enter in the identity information of the P-AI header. The maximum length of this field is 50 digits. If you enter more than 50 digits , enter other characters, or leave this field blank, SMI displays a warning when you save the updates to the Sites page.

Table continues…

Name	Description
Always use site configured name and number	The option to enable or disable Messaging from always using the default identity information of the site for the P-AI header. • Select this check box to enable Messaging to always use the default identity information of the site for the P-AI header. • Clear this check box to disable Messaging from always using the default identity information in the P-AI header and enable Messaging to determine the identity information in the P-AI header based on the feature that is used in the call. For example, Reach Me and Auto Attendant. When you create a new site, this check box is not selected by default.

Operator (Live Attendant)

Name	Description
Availability	The option to indicate the availability of the attendant. 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 if the attendant is unavailable.

Auto Attendant

Name	Description
Auto Attendant	The option to enable or disable the Auto Attendant feature. The default value is **disabled**. Auto Attendant transfers callers to local extensions with associated mailboxes.

Table continues…

Name	Description
Pilot Number	The pilot number for Auto Attendant. You can configure up to 10 Auto Attendant pilot numbers for each site. Each Auto Attendant number supports up to three languages. Each pilot number and language group setting represents an Auto Attendant language selection menu for that pilot number. For example, Site 1 with: • **Short extension length**: 4 • **Extension style for telephony integration**: E.164 • **Site Identifier** = 1899 • Already created **AA pilot number** = 3333 (i.e. the prefixed AA pilot number for Site 3 = 18993333)
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. Messaging associates the selected Auto Attendant language with all users who belong to the site. The default language that is associated with each Auto Attendant is English-US, which is also the default system language.
Additional Language	The languages that you installed on the application server associated with a site. Use the two options to select two additional languages for the Auto Attendant number associated with a site. By selecting additional languages, users can select a language with one multilanguage greeting. The user can choose a language from maximum three languages.
Additional sites included in the directory	The name of another site in a multisite deployment. Each site has an 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. Click 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 contacts the users who are in both the directories through Auto Attendant for this site. If you change the selections in this field, you must reload User List on all application servers for the site or wait for the nightly refresh for the changes to take effect.

Table continues…

Name	Description
Keypad entry	The keypad options are: • **BASIC**: Enter extension only. • **ENHANCED**: Enter the extension number or spell the name of the user. If the **Speech recognition** field is *enabled*, both options include speech recognition.
Speech recognition	The option to enable speech recognition. With speech recognition, users can call a person whose name exists in the Auto Attendant directory by uttering the name of the person. Auto Attendant transfers the call to the person. This option is active only if you administer the same default language for all sites in Auto Attendant. The default value of this option is *disabled*. Do not enable this feature unless your Messaging system includes a mainstream license. **Important:** If you enable speech recognition for a site, ensure that the application server that hosts the site does not have more than three language packs installed. If you exceed this limit, you might exhaust the memory capacity.
The maximum number of speech recognition results	The option to administer the number of users that Messaging suggests through the speech recognition feature. You can administer Messaging to suggest up to nine users.
Allow transfer to non-native mailbox extensions	The option using which Auto Attendant transfers callers to non-native mailbox extensions.

Auto Attendant Greeting / Menu

Name	Description
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 (keypad entry is basic):	The menu that Auto Attendant plays when you set **Keypad entry** to **basic**.
Menu (keypad entry is enhanced):	The menu that Auto Attendant plays when you set **Keypad entry** to **enhanced**.

Button	Description
Play	Provides an interface to download the .wav file from the server to the personal computer of the user.
Browse	Launches a file selector window.
Upload (Replace Current)	Uploads the selected .wav file.
Restore Default	Uploads the default .wav file.

Call Answering Greeting

Name	Description
System greeting before call answering	The optional system greeting that Messaging plays before the external and internal greeting. You can use the system greeting to play additional messages such as standard disclaimers.

Button	Description
Play	Provides an interface to download the .wav file from the server to the personal computer of the user.
Browse	Launches a file selector window.
Upload (Replace Current)	Uploads the selected .wav file.
Restore Default	Uploads the default .wav file.

Related links

P-AI header value for features on page 67

P-AI header value for features

You can customize the identity information in the P-AI header value. The caller ID that a called user receives might be different than what you administer in the P-AI headers.

Earlier Messaging releases did not support custom identity information, so the other components in the network determined the values of the P-AI headers.

Depending on the feature that starts the outbound call and the availability of the incoming caller ID, Messaging determines the P-AI header value.

- Caller: Sets the P-AI header value based on the incoming call.
- Subscriber: Sets the header value based on the value administered for the extension of the user.
- Site: Sets the header value based on the value administered for a site.

Feature	Incoming Caller ID provided	No caller ID provided
Auto Attendant	Caller	Site

Table continues…

Feature	Incoming Caller ID provided	No caller ID provided
Personal Operator	Caller	Site
Reach Me	Subscriber	Subscriber
Caller Applications	Caller	Site
Call Sender	Subscriber	Subscriber
Notify Me	None	Subscriber
Diagnostics	None	Configurable
Fax Send	None	Subscriber
Audix *T	None	Subscriber
Play on Phone	None	Subscriber

Related links

Sites field descriptions on page 53

Regular expressions for phone number translation rules

Pattern	Meaning
0123456789	Literal digits.
\d	Any digit.
*	Zero or more repetitions of the preceding regular expression.
+	One or more repetitions of the preceding regular expression
?	Zero or one repetitions of the preceding regular expression.
[...]	Any of the enclosed set of digits, for example, [12] would match either “1” or “2” digit, but not any other digit.
{ m }	Exactly m repetitions of the preceding regular expression, so 12{3} would match 1222.
{ m ,}	m or more repetitions of the preceding regular expression.
{ m , n }	Between m and n repetitions of the preceding regular expression.

The examples are as below:

- 1{2} [1–38] \d {4} : 7 digit numbers starting with 111, 112, 113 or 118.
- 2?3 {2} [0–9] {4,5} : 7–8 digit numbers starting with 233 or 6–7 digit numbers starting with 33.
- 8*\d{5} — 5 and more : digit numbers starting with 0 or more 8’s.

Setting the length of the mailbox number

Before you begin

Ensure that Messaging is running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Storage)** > **Networked Servers**.
2. On the Manage Networked Servers webpage, select the server and click **Edit the Selected Networked Server**.
3. From the **Mailbox Number Length** drop-down list:
   - To set mailbox numbers with different lengths, select **Variable**.
   - To set a fixed length for the mailbox number, select a number that corresponds to the length of the mailbox extension used by your system.

   Messaging displays the following message:

   ```
   You must provide a password for the networked server.
   ```
4. Type the password for the server, and confirm the password.

   Note the password that you enter in the **Password** and **Confirm Password** fields. You must enter this password when you want to administer point-to-point networking between:
   - Messaging servers.
   - Messaging servers and Message Networking servers.
5. Click **Save**.

Next steps

Administer the IMAP4 access to the storage server.

Add the postmaster mailbox.

Related links

Configuring IMAP4 access on page 69
Adding the postmaster mailbox on page 70

Configuring IMAP4 access

About this task

Configure systemwide parameters on the System Administration webpage. 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

Ensure that Messaging is running.

Procedure

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

Next steps

Administer the system mailboxes.

Related links

Adding the postmaster mailbox on page 70
System Administration field descriptions on page 159

Adding the postmaster mailbox

About this task

The postmaster mailbox manages the voice mail and the email delivery for the entire system. This mailbox, which is integral to Messaging, is an internal system mailbox. The postmaster mailbox number must be a unique number. Select a mailbox number that has the same length as the subscriber mailbox numbers.

Before you begin

Ensure that Messaging is running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. In the **Add User / Info Mailbox** area, in the **Add a new user**, click **Add** to add a new user.
3. On the User Management > Properties for New User webpage:
   - In **Last name** field, type `postmaster`.

     Important:

     You must enter `postmaster` in the lowercase.
   - In the **Site** field, click **Default**.
   - In **Mailbox number** field, type a unique mailbox number for the postmaster.

- In **Extension** field, type the extension of the postmaster.

The length of the mailbox number and the extension must match the length that you specified in *Setting the length of the mailbox number*.

4. Select **Postmaster** as CoS.
5. Set **MWI enabled** to **No**.
6. Turn off the following defaults:
   - **Include in Auto Attendant directory**
   - **User must change voice messaging password at next logon**
7. Complete the following password fields:
   - **New password**
   - **Confirm password**
8. Click **Save**.

   The system creates a site-wide mailbox.

Next steps

Define the mailbox that you created as the postmaster mailbox.

Related links

Setting the length of the mailbox number on page 69
Configuring the postmaster mailbox number on page 71
User Management > Properties field descriptions on page 194

Configuring the postmaster mailbox number

About this task

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

The system does not count the postmaster mailbox in the total number of user licenses that your organization bought.

Before you begin

- Create a mailbox for the postmaster.
- Ensure that Messaging is running.

Procedure

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

3. Click **Save**.

Next steps

- Create a shadow mailbox for the distribution of ELA messages.
- Configure a flexible storage.

Related links

Adding the postmaster mailbox on page 70
Creating a shadow mailbox on page 72
Flexible storage on page 81

Creating a shadow mailbox

About this task

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. In the **Last name** field, type a descriptive name.

   For example, `shadow_do_not_reply`.
5. In the **Site** field, click **Default**.
6. In the **Mailbox number** field, type the number.
7. In the **Extension** field, type the extension number.

   The extension must match the entry in the **Mailbox number** field.
8. Select **ELA** as CoS.
9. In the **New password** field, type the password.
10. Confirm the password in the **Confirm password** field.
11. Click **Save**.

Next steps

Configure the shadow mailbox on the System Mailboxes webpage.

Related links

User Management > Properties field descriptions on page 194

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.
3. Click **Save**.

Next steps

Administer SMTP.

Related links

Administering the external SMTP host on page 76
System Mailboxes field descriptions on page 74

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

Adding the broadcast mailbox

About this task

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

Before you begin

Ensure that Messaging is running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. In the **Add User/Info Mailbox** area, in the **Add a new user**, click **Add**.
3. On the User Management >Properties for New User webpage, perform the following:
   - In the **Last name** field, type `broadcast`.
   - In the **Site** field, click **Default**.
   - In the **Mailbox number** field, type a unique mailbox number for the broadcast.
   - In the **Extension** field, type the extension of the broadcast.

     The length of the mailbox number and the extension must match the length that you specified in *Setting the length of the mailbox number*.
4. In the **Class of Service** field, select the class of service name that you want to assign for this broadcast mailbox.

5. Set **MWI enabled** to **No**.
6. Turn off the following defaults:
   - **Include in Auto Attendant directory**
   - **User must change voice messaging password at next logon**
7. Complete the following password fields:
   - **New password**
   - **Confirm password**
8. Click **Save**.

   The system creates a broadcast mailbox.

Next steps

Configure the broadcast mailbox number.

Configuring the broadcast mailbox number

About this task

After you create a mailbox for the broadcast, identify the mailbox as the broadcast mailbox.

Before you begin

- Ensure that Messaging is running.
- Create a mailbox for the broadcast.

Procedure

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

System Mailboxes field descriptions

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

Name	Description
SYSTEM MAILBOXES	

Table continues…

Name	Description
Internet Postmaster Mailbox Number	The number for the internet postmaster master 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 and is integral to the operation of the Messaging system.
Enhanced-List Application Shadow Mailbox Number	The mailbox number for the ELA shadow mailbox. The administrator configures the ELA shadow mailbox to create distribution lists for delivering messages.
Broadcast Mailbox Number	The mailbox number of the local user created to store broadcast messages before they are delivered to all other users.
DEFAULT ENHANCED-LIST ATTRIBUTES	
List Mailbox Default Class-of-Service	The default value of the Class-of-Service for enhanced-lists.
List Mailbox Default Community ID	The default value of the Community Id for enhanced-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 webpage.
Broadcast Message Active Time (Days)	The number of days for which a broadcast message remains active until the message is deleted or a new broadcast message is recorded.
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.

Enable outbound SMTP based traffic

Administering the external SMTP host

About this task

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 webpage.

Note:

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

Before you begin

Ensure that 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**.

Next steps

Administer a mail gateway to connect to other mail applications.

Related links

Adding a mail gateway on page 77

Add a New External Host field descriptions

Name	Description
IP Address	The IP address of the external SMTP server.

Table continues…

Name	Description
Host Name	The host name of the external SMTP server. **Note:** If the external server is in a different domain than the AAM domain, then you must enter the fully qualified domain name for the external host. For example, galsil-exch.interop.com.
Alias	The alias of the external SMTP server. This field is optional.

Adding a mail gateway

About this task

Use Messaging to add a mail gateway to connect to other mail systems and send text messages from the storage server.

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*.
3. In the **Mailbox Gateway Machine Port** field, enter a port number to connect to the selected mailbox gateway.
4. Keep the **Server Alias** field blank.
5. Click **Save**.

Next steps

- Change the LDAP root password for the internal LDAP processes.
- Administer a storage server.

Related links

Changing the LDAP root password on page 78
Administering the external SMTP host on page 76
Configuring a storage destination on page 79
Network overview on page 22
Mail Options field descriptions on page 393

Changing the LDAP root password

About this task

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 webpage.

2. If you want to start a shutdown, click **Stop**.

   The Stop Messaging Software webpage 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. Messaging might take a few seconds to display the 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.

   Some browsers automatically populate web-based forms with passwords. If **New password** contains a value, clear the field and enter the password. To prevent Messaging from automatically populating the passwords, turn off the option to remember the password in your browser.

8. Enter the new password again in the **Confirm New Password** field.

9. Click **Save**.

   If you do not enter a new password in Step 7 and Step 8, your browser displays the following error after you click **Save**:

   ```
   You must enter a password.
   ```

10. On the **Administration** menu, click **Messaging** > **Utilities** > **Start Messaging**.

    The system displays the Start Messaging Software webpage.

    The Start Messaging Software webpage 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. Messaging might take a few seconds to display the message.

11. Click **OK**.

Next steps

If you use Exchange Server, administer a storage server.

Related links

Configuring a storage destination on page 79
Flexible storage on page 81

Configuring a storage destination

About this task

Use this procedure to configure Exchange Server as the storage destination.

The Avaya message store does not require any configuration.

Before you begin

Configure the mail host.

Procedure

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

   The system displays the Storage Destinations webpage.

2. Enter the appropriate information in the fields to define the required service account.
3. Click **Save**.

   Messaging tries to log in to the account and checks that a corresponding mailbox is created for that account. If either test fails, then the system displays an error.

   External storage destinations require specific settings on the System Administration webpage. If you enable Exchange Server as your message store in Step 2 and save the changes, Messaging displays a message and sets the following values:

   - **Privacy Enforcement Level**: Email
   - **Automatic Mail Forwarding**: yes

4. Click **OK**.
5. Restart Messaging for the changes to take effect.

Next steps

- Administer Exchange Server as a flexible storage.
- Select the storage destination for users.

Related links

Adding a mail gateway on page 77

Stopping Messaging on page 460
Starting Messaging on page 460
Selecting a storage destination on page 102
Flexible storage on page 81
Storage Destinations field descriptions on page 80

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.	
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. 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 SSL to access Global Catalog	The option to use the Secure Sockets Layer (SSL) encryption for secured access to the Global Catalog.

Table continues…

Name	Description
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 dc1.avaya.com.

Related links

Initial administration checklist for the storage role on page 40

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 message store is a built-in storage.
- Microsoft Exchange Server: Messaging supports Exchange Server 2007, 2010, and 2013 as a message store. Messaging does not support Exchange 365. Messaging supports Active Directory provisioning. You can use the Active Directory look-up utility to import user data into the Messaging directory. From the telephone data of Active Directory, you can get user properties, such as information about mailboxes, the extension numbers, and the sites. If you use the existing Active Directory, Messaging can gain access to the most relevant user data, such as the name or the telephone numbers.

You can designate a storage server to each user. This flexibility supports the dual environment of the Avaya message store and the Exchange Server email servers.

Service account and permissions

If you use the Avaya message store as a storage server, you do not need to configure the message store.

If you use Exchange Server as a storage server, you must:

- Create a mailbox for the Messaging service account on Exchange Server.

  Provide the Exchange Server Impersonation privileges to the service account. Exchange Server processes the service account as an Active Directory Domain User account with an Exchange Server mailbox. With the Impersonation privileges, a caller can impersonate an account so that the caller can perform operations by using the permissions of the impersonated account.

- Configure Exchange Web Services (EWS) on Exchange Server. With EWS, client applications can communicate with the Exchange Server through web services. EWS

provides access to almost all data that is available through Microsoft Office Outlook. You must configure EWS to ignore client certificates and enable one of the authentication types supported by Messaging.

- Configure Exchange Autodiscover service on Exchange Server. With Autodiscover, EWS clients can find EWS endpoint URL without specifying it manually. You must configure Autodiscover to ignore client certificates and enable one of the authentication types supported by Messaging.

  Messaging supports the following authentication types for EWS and Autodiscover:

  - Basic Authentication
  - NTLM (NT LAN Manager) Authentication

  Note:

  Messaging always uses Transport Layer Security (TLS 1.2) to secure communication with EWS.

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.

Microsoft Exchange Server 2007

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 authentication for EWS on Exchange Server 2007 running Windows server 2003

Procedure

1. Open **Internet Information Services (IIS) Manager**.
2. In the left pane, click **Web Sites** > **Default Web Site**.
3. Right click **EWS**, and click **Properties**.
4. In the EWS Properties dialog box, click the **Directory Security** tab.
5. In the **Authentication and access control** section, click **Edit**.
6. In the **Authenticated Access** section, select the following:
    a. **Basic Authentication (password is sent in clear text)**
    b. **Integrated Windows authentication** for NTLM authentication.

Configuring authentication for Autodiscover on Exchange Server 2007 running Windows server 2003

About this task

Use this procedure to configure Autodiscover on Exchange Server 2007.

Procedure

1. Open **Internet Information Services (IIS) Manager**.
2. In the left pane, click **Web Sites** > **Default Web Site**.
3. Right click **Autodiscover**, and click **Properties**.
4. In the Autodiscover Properties dialog box, click the **Directory Security** tab.
5. In the **Authentication and access control section**, click **Edit**.
6. In the **Authenticated Access** section, select the following:
    a. **Basic Authentication (password is sent in clear text)**
    b. **Integrated Windows authentication** for NTLM authentication.

Granting the relay permission to anonymous connections for Exchange Server 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. In the **Specify the FQDN this connector will provide in response to HELO or EHLO** field, enter FQDN of Exchange Server.
   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. Replace the **0.0.0.0 - 255.255.255.255** IP address range with the Messaging IP address. For example, 103.20.74.46 — 103.20.74.46.
   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**.

Microsoft Exchange Server 2010

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.

Configuring authentication for EWS on Exchange Server 2010 running Windows server 2008

Procedure

1. Open the **Internet Information Services (IIS) Manager**.
2. In the Connections pane, click **Sites** > **Default Web Site** > **EWS**.
3. In **Features View**, double-click **Authentication**.
4. On the Authentication page, right-click the following:
   a. **Basic Authentication**: Click **Enable** for Basic authentication.
   b. **Windows authentication**: Click **Enable** for NTLM authentication.

Configuring authentication for Autodiscover on Exchange Server 2010 running Windows server 2008

About this task

Use this procedure to configure Autodiscover on Exchange server 2010.

Procedure

1. Open **Internet Information Services (IIS) Manager**.
2. In the Connections pane, click **Sites** > **Default Web Site** > **Autodiscover**.
3. In **Features** view, double-click **Authentication**.
4. On the Authentication page, right-click the following:
    a. **Basic Authentication**:Click **Enable** for Basic Authentication.
    b. **Windows authentication**: Click **Enable** for NTLM authentication.

Granting the relay permission to anonymous connections for Exchange Server 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. In the **Specify the FQDN this connector will provide in response to HELO or EHLO** field, enter FQDN of Exchange Server.
    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. Replace the **0.0.0.0 - 255.255.255.255** IP address range with the Messaging IP address. For example, 103.20.74.46 — 103.20.74.46.

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**.

Microsoft Exchange Server 2013

Administering the impersonation permission for Exchange Server 2013

About this task

Provide the impersonation permission to the service account of each Exchange Server that functions as Client Access Server (CAS).

Note:

The service account to which you provide the impersonation permission must not be a member of any Administrative Group, such as Domain Admins, because Messaging denies the application impersonation permission to these groups. Use an account with Domain Administrator credentials and administrative credentials for the computers on which you installed the Exchange 2013 Client Access Server roles to provide the permission.

Before you begin

Ensure that:

- You create the Messaging service account.
- Active Directory (AD) has an alias record for the domain of the Exchange Server, such as aamdomain.ca.avaya.com

Procedure

1. Log in to Exchange admin center using the following URL: https://<Exchange server>/ECP.
2. Click **permissions** > **admin roles**.
3. To add a new role group, click the plus sign (+).

   Exchange admin center opens the new role group window.

Note:

If you use Internet Explorer, the browser might block pop-ups from Exchange admin center. To disable Pop-up Blocker, click **Tools** > **Internet Options** and clear the **Turn-on Pop-up Blocker** check box on the **Privacy** tab.

4. Enter the appropriate information in the fields and assign the **ApplicationImpersonation** role to the role group.
5. Click **Save**.

Related links

Creating the Messaging service account on page 82

Configuring authentication for EWS on Exchange Server 2013 running Windows Server 2012

Procedure

1. Open the **Internet Information Services (IIS) Manager**.
2. In the Connections pane, click **Sites** > **Default Web Site** > **EWS**.
3. In **Features View**, double-click **Authentication**.
4. On the Authentication page, right-click the following:
   a. **Basic Authentication**: Click **Enable** for Basic authentication.
   b. **Windows authentication**: Click **Enable** for NTLM authentication.

Configuring authentication for Autodiscover on Exchange Server 2013 running Windows Server 2012

About this task

Use this procedure to configure Autodiscover on Exchange Server 2013.

Procedure

1. Open the **Internet Information Services (IIS) Manager** .
2. In the Connections pane, **Sites** > **Default Web Site** > **Autodiscover**.
3. In **Features** view, double-click **Authentication**.
4. On the Authentication page, right-click the following:
   a. **Basic Authentication**: Click **Enable** for **Basic Authentication**.
   b. **Windows authentication**: Click **Enable** for NTLM authentication.

Administering the relay permission to anonymous connections for Exchange Server 2013

Procedure

1. Log in to Exchange admin center using the following URL: `https://<Exchange server>/ECP`.
2. Click **mail flow** > **receive connectors**.
3. Select **Default Frontend** and click the pencil icon to edit the default receive connector.

   Exchange admin center opens the Default Frontend window.

   Note:

   If you use Internet Explorer, the browser might block pop-ups from Exchange admin center. To disable Pop-up Blocker, click **Tools** > **Internet Options** and clear the **Turn-on Pop-up Blocker** check box on the **Privacy** tab.
4. Click **security** and select the **Anonymous users** check box.
5. Click **Save**.

Configuring MWI

MWI administration

From Release 7.0.0, the MWI functionality is moved from the Application servers to the Message Storage Server.

You must administer your existing telephony integration and add the address of the storage server to the Messaging SIP entity on System Manager.

Note:

Perform this task only on the storage-only server.

Enabling SIP telephony integration

Procedure

1. Log in to Messaging System Management Interface.
2. In the **Administration** menu, click **Messaging** > **Telephony Settings** > **Telephony Integration**.
3. In the **Switch Integration Type** field, select **SIP**.

4. Enter the appropriate information in the fields.
5. Click **Save**.
6. Restart Messaging.

Telephony Integration field descriptions

BASIC CONFIGURATION

Name	Description
Switch Integration Type	The type of switch integration that Messaging uses. The SIP SPECIFIC CONFIGURATION section is available only for SIP integration.

SIP SPECIFIC CONFIGURATION

SMI displays the following section only if you click **SIP** in the **Switch Integration Type** field. On the Telephony Integration page, you have read-only access to these fields. You can administer these fields on the Telephone Domains page.

Name	Description
Far-end Domains	The number of far-end SIP domains. SMI displays the number of rows that are equal to the number of far-end SIP domains that you select from the drop-down list. You can add maximum 500 SIP domains.
SIP Domain	The domain names of the application server and the far-end connection. For example, sip.example.com. • **Telephony Profile Name**: The name of the telephony profile that represents a gateway ID and SIP domain of the application server. • **Gateway ID**: The ID of the far-end connection gateway. • **Messaging SIP domain**: The name of the Messaging SIP domain. • **Far-end domain**: The name of the far-end SIP domain connection.
Far-end Connections	The number of connections to the far-end SIP proxy servers. SMI displays the number of rows that are equal to the number of far-end SIP domains that you select from the drop-down list. You can add maximum 25 far-end connections.

Table continues…

Name	Description
Connection	The connection details of a far-end connection that includes: • **Gateway ID**: The ID of the far-end connection gateway. • **IP**: The IP address of the connection. • **TCP or TLS**: The transport method that the telephony server uses for SIP signaling. The transport method of the application server and the telephony server must match. The types of transport methods are: - **TCP**: Not encrypted. - **TLS**: Encrypted. • **Port**: - **TCP**: 5060 - **TLS**: 5061 • **Monitor interval**
Messaging IPv4 Address	The address of the near-end application server. This address is always a read-only field. • **IP**: Use the IP address of the server. • **TCP Port**: Use port 5060. • **TLS Port**: Use port 5061.
Messaging Ports	The maximum number of active calls to or from a user. • **Call Answer Ports**: The range of the ports, which is from 2 to 100. • **Maximum**: The maximum number of ports that Messaging uses. • **Transfer Ports**: The maximum number of transfer ports that Messaging uses.

Table continues…

Name	Description
Switch Trunks	The number of trunk members for Messaging on the telephony server. • **Total**: The total number of trunks administered. Messaging requires at least one more port than the number of ports that you administer in **Call Answer Ports**. • **Maximum**: The telephony server supports maximum 120 trunk members. The trunk members, in addition to the call answer ports, are for features such as the transfer feature, which require more switch trunks. If the telephony server specifies the maximum number of trunks, the number in the **Switch Trunks** field must match the number on the telephony server.

ADVANCED OPTIONS

When the ADVANCED OPTIONS section is hidden, SMI displays the **Show Advanced Options** button. When you click **Show Advanced Options**, the button changes to **Hide Advanced Options** and SMI displays the ADVANCED OPTIONS fields.

Name	Description
Quality Of Service	The QoS field to administer: • **Call Control PHB**: The quality of service level for call control messages. • **Audio PHB**: The quality of audio streams. Use this field if your IP network infrastructure supports QoS. You can keep the default values in QoS or enter new values. The values you enter must match the number in the network region of the telephony server. This is the telephony server that the Messaging signaling group uses. The range for both these fields is 0 to 63.
UDP Port Range	The range of port numbers used by UDP for RTP. The default range is 8000 to 10000. • You can change the **Start** value. • Messaging 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 the ports used for other purposes.

Table continues…

Name	Description
G.729 Codec Support	The option to enable support for the G.729 codec for media transmission. • If you select this check box, Messaging supports the G.729 and G.729A codecs with the G.711 μ-law and G.711 A-law codecs. • If you clear this check box, Messaging only supports the G.711 μ-law and G.711 A-law codecs. **Note:** Messaging supports the G.711 and G.729 codecs only for media transmission. Messaging supports the GSM codec and the G.711 codec for storage encoding.
Minimum TLS Version	The minimum TLS version that the telephony server uses for SIP signaling on the TLS port. The default TLS version is 1.0. Ensure that all far-end SIP proxy servers support the selected TLS version or higher.
Media Encryption	The type of SRTP media encryption that the telephony server uses. This field is optional. **Note:** The storage server must be online for the media encryption-related changes to take effect. If you have a single-server installation, Messaging must be running.
Enforce SIPS URI for SRTP	The option to specify whether a SIPS URI or secure URI is required for SRTP. If you set the value to **yes**, then any incoming call that contains SRTP without a SIPS URI fails.
SIP INFO for DTMF	The SIP INFO messages for the out-of-band DTMF. The options are: • **Ignore**: Ignore all SIP INFO DTMF digits in the signaling stream. This is the default value. • **Accept**: 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 milliseconds.

Table continues…

Name	Description
Include “AAM” in From/P-AI Header	The option to add “AAM” in the From SIP header and P-Asserted Identity SIP header.
Media Encryption During CapNeg	The SRTP media encryption that the telephony server uses when capability negotiation (CapNeg) is present in SDP. The options are: • **Enabled**: Set the default value. • **Disabled**: Change the value in the **Media Encryption** field to **None**. Messaging automatically changes the value, and you cannot change the value. Select **Disabled** only for a specific telephony integration. For more information about administering the media encryption during CapNeg, see the configuration notes.
Supported Header includes “replaces”	The supported header that must include the *replaced* value so that endpoints reflect the capabilities in SIP headers and Messaging effectively communicates with a specific telephony integration. The options are: • **no**: The default value. • **yes**: Only for a specific telephony integration. For more information about administering the header with the *replaces* value, see the configuration notes.
Telephone Event Payload Type	The RTP payload type for RFC2388 DTMF events. The dynamic payload type range is *96* to *127*. The default value is *127*. For example, when Messaging starts a call for a Reach Me operation, Messaging specifies the *127* RTP payload type for RFC2388 DTMF events. This field is inactive if you set the SIP INFO for DTMF field to *Accept*.

Table continues…

Name	Description
Monitor Far-end OPTIONS messages	The option to enable Messaging to proactively monitor the SIP OPTIONS messages that the far-end connection sends. If Messaging does not receive a SIP OPTIONS message from the far-end within the time specified in the **Proactive Interval** field, Messaging considers the far-end as nonfunctional or unreachable. The options are: • **no**: Disables monitoring of the OPTIONS messages. This is the default value. • **yes**: Enables monitoring of the OPTIONS messages. • **Proactive Interval**: The interval, in seconds, for which the far-end is configured for sending the OPTIONS message.
Inactive Link Actions	The option to generate an alarm or disconnect all incoming connections. The options are: • **Alarm Only**: Messaging generates an alarm when an expected OPTIONS message does not arrive within the interval configured in **Proactive Interval** + 30% of the interval period. For example, if you configure the interval as 10 seconds, Messaging generates an alarm after 10 + 3 (30% of 10) = 13 seconds. On the next successful receipt of SIP OPTIONS or the next incoming call, Messaging clears the alarm. • **Close Connections**: Messaging generates an alarm, closes all incoming connections, and drops all active calls. This option is only available if you set the value of **Monitor Far-end OPTIONS messages** to **yes**.
Minimum Session Refresh Interval	The minimum session refresh interval in seconds. Usually, the refresh interval value is set to match the interval value administered for the switch.
SIP REFER Delay	The delay of the transfer operation in milliseconds when a Messaging outbound call is answered and the SIP REFER request sent. The value range is 0 to 5000 milliseconds.
Minimum Fax Power Threshold	The minimum power level threshold to detect the incoming CNG fax tone. The value range is 14000 to 1400000. The default value is 140000.

Table continues…

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: • P-Asserted Identity • Multiple SIP domains • SIP UUI
Cross-Switch Transfer	The option to enable and disable call transfers between different gateways. Cross-switch transfer is enabled by default.
Connection Audits	The option to enable the audit of the incoming, the outgoing, and the MWI SIP connections. By default, Messaging disconnects the connections that are idle for 30 minutes.
Customize Blocked Caller-ID	The option to customize the appearance of the blocked caller ID with a customized caller ID. This check box is clear by default. **Important:** To determine how the system displays the customized caller ID, check with your service provider. You can understand how the network of the service provider processes a blocked caller ID.

Table continues…

Name	Description
Blocked Caller-ID	The option to administer values to at least one of the following fields to customize the caller ID appearance: • **Username** • **Display Name** These fields are available if you select the **Customize Blocked Caller-ID** check box. • The user name and the display name: anonymous@anonymous.invalid • Only the user name: anonymous@anonymous.invalid • The user name with the SIP domain: anonymous-sip.com
Blocked Caller-ID Matches	The option to administer the SIP headers that Messaging examines to determine whether the caller ID of the incoming call is blocked. The options are: • **From Header**: To administer Messaging to examine the From SIP header. • **P-AI Header**: To administer Messaging to examine the P-Asserted Identity SIP header.

Related links

Support for SIP INFO messages on SIP connections on page 133

Creating a SIP entity of a storage server on System Manager

About this task

Use this procedure to create a SIP entity.

Procedure

1. On the home page of the System Manager web console, in **Elements**, click **Routing** > **SIP Entities**.
2. Click **New**.
3. In the General window, do the following:
   a. In the **Name** field, type the name of the SIP entity.
   b. In the **FQDN** or **IP Address** field, type the FQDN or IP address of the SIP entity.
   c. In the **Type** field, select **Messaging** as the type of the SIP entity.
   d. In the **Notes** field, type information about the SIP entity.
   e. In the **Location** field, click a location.

f. In the **Time Zone** field, click the default time zone for the SIP entity.

g. In the **Credential name** field, type a regular expression string.

For example: To use `www.sipentity.domain.com`, type the string `www\.sipentity\.domain\.com`.

4. Click the appropriate mode in **Loop Detection Mode**.

The default value of **Loop Detection Mode** is **On**.

5. In the **SIP Link Monitoring** field, click one of the following:

- **Use Session Manager Configuration**
- **Link Monitoring Enabled**
  - In the **Proactive Monitoring Interval (in seconds)** field, type the time. The range is 1 to 9000 seconds, and the default value is 900.
  - In the **Reactive Monitoring Interval (in seconds)** field, type the time. The range is 1 to 900 seconds, and the default value is 120.
  - In the **Number of Tries** field, type a number. The range is 0 to 15, and the default value is 1.
- **Link Monitoring Disabled**

6. To specify the Entity Links:

a. Click **Add**.

b. In the **Name** field, type the name.

c. In the **SIP Entity 1** field, click the required Session Manager SIP Entity.

SIP Entity 1 must always be a Session Manager instance.

d. In the **Protocol** field, click the appropriate protocol.

e. In the **Port** field, type the required port.

f. In the **SIP Entity 2** field, click the required non-Session Manager SIP Entity.

g. In the **Port** field, type the required port.

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

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

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

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

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

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

8. To specify the Port parameters:
    a. Click **Add** in the Port section.
    b. Enter the necessary port and protocol parameters
9. **(Optional)** To remove an incorrectly added Port, click the respective **Port** and click **Remove**.
10. For OPTIONS requests, in the **Response Code & Reason Phrase** field, add or remove a SIP code and phrase to mark the SIP entity as up or down, respectively.
11. Click **Commit**.

Creating a single SIP entity of a storage server

About this task

Use this procedure to create a single SIP entity for Avaya Aura® Messaging storage server.

Procedure

1. On the home page of the System Manager web console, in **Elements**, click **Routing** > **SIP Entities**.
2. Click **New**.
3. In the General window, do the following:
    a. In the **Name** field, type the name of the SIP entity.
    b. In the **FQDN** or **IP Address** field, type the FQDN or IP address of the SIP entity.
    c. In the **Type** field, select **Messaging** as the type of the SIP entity.
    d. In the **Notes** field, type information about the SIP entity.
    e. In the **Adaptation** field, click the adaptation.
    f. In the **Location** field, click a location.
    g. In the **Time Zone** field, click the default time zone for the SIP entity.
    h. In the **SIP Timer B/F (in seconds)** field, enter the time in seconds.
    i. In the **Minimum TLS Version** field, click select the TLS version.
    j. In the **Credential name** field, type a regular expression string.

    For example: To use `www.sipentity.domain.com`, type the string `www \.sipentity\.domain\.com`.
    k. In the **Call Detail Recording** field, click **none**.
4. In the Loop Detection window, do the following:
    a. Click the appropriate mode in **Loop Detection Mode**.

    The default value of **Loop Detection Mode** is **On**.

b. In the **Loop Count Threshold** field, type the loop count threshold value.

c. In the **Loop Detection Interval (in msec)** field, enter the value of loop detection interval.

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

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

      This is the port on which you have configured the remote entity to receive requests for the specified transport protocol.
   h. In the **Connection Policy** field, click the appropriate policy.

      Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
   i. Click **Deny New Service** to deny service for the associated entity link.
7. **(Optional)** In the **Failover** field, add ports if the SIP entity is a failover group member.

   This step is applicable only for Session Manager SIP entity type.
8. To specify the Port parameters:
   a. Click **Add** in the Port section.
   b. Enter the necessary port and protocol parameters
9. **(Optional)** To remove an incorrectly added Port, click the respective **Port** and click **Remove**.

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

Creating local host name entries for storage server

About this task

Use this procedure to add local host name entries for storage server.

Procedure

1. On the home page of the System Manager web console, in **Elements**, click **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. In the New Local Host Name Entries section, do the following:
   a. In the **Host Name (FQDN)** field, type the FQDN of SIP entities.
   b. In the **IP address** field, type the IP address.
   c. In the **Port** field, type the value of the port.
   d. In the **Priority** field, set the priority.
3. Click **Commit**.

Selecting a storage destination

About this task

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

Caution:

If you change the storage destination for an existing user, the existing voice messages remain in the original message store and are unavailable for review through 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. Perform one of the following tasks:
   - To locate an existing user, in the **Identifier** field, enter a user 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.

4. Select a storage destination from the **Storage destination** drop-down list.

   If you select Exchange Server as your storage destination to support the Exchange Server users, the system enables the **Automatic Mail Forwarding** field in the System Administration webpage.

5. In the **Exchange email address** field, enter the email address of the Exchange Server 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.

Related links

Initial administration checklist for application roles on page 105
User Management > Properties field descriptions on page 194

Verifying the status of the storage role

About this task

The System Status webpage displays the status of the following processes:

- Message Store
- Other enabled software modules such as:
  - Enhanced-List Administration
  - Internet Messaging
  - LDAP processes
  - The available hours of speech. Use the number of hours to determine if the system has enough space for recording voice messages.

Note:

After you migrate data from another Messaging system, ensure that the **User Data Migration** process is in the *Not Running* state before restarting Messaging.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Information** > **System Status**.

   Messaging displays the results.

2. To view the updated results, click **Refresh**.

Chapter 5: Initial administration of the application role

Deployment scenarios

Use the instructions in this chapter 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 might need to perform some tasks multiple times. Use the following scenarios and the initial administration checklist to plan your administration activities.

The following deployment scenarios relate to the tasks in *Initial administration checklist for application roles*. For more information about deployment options, see *Avaya Aura® Messaging Overview and Specification*.

One server and one site

Associate one application role with a site by completing the tasks in the initial administration checklist.

Multiple servers and one site

Associate more than one application role with one site. For example, your topology might be a site in Atlanta that has three dedicated application servers.

For this example, complete all tasks on the three dedicated application servers.

Multiple servers and multiple sites

Associate multiple application roles to each site.

For example, if your topology has:

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

For this example, complete all tasks on the three dedicated application servers in Atlanta and one application server in Boston.

Important:

Do not restore the backup of system files of a site on application servers associated with a different site.

Initial administration checklist for application roles

Use the following checklist to set up application roles for the first time. In large organizations with specialized administration roles, the Messaging administrator usually performs these tasks.

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 and restore the backup data on subsequent application servers.

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

No.	SMI page	Task	On the first application server of the first site	On the first application server of the subsequent site	On the subsequent server in any site
1	Server Role / AxC Address	Administering the server role and AxC IP address on page 42.	Yes	Yes	Yes
2	Dial Rules	Administering dial rules on the application server on page 105.	Yes	Yes	Yes
3	Cluster	Configuring a cluster on page 110. Perform this task only if you add more application servers.	—	Each application server in the cluster	—
4	System Parameters	Enabling fax on page 112.	Yes	Yes	No
5	Language Packs	Configuring languages on page 115.	Yes	Yes	Yes
6	Network Configuration	Configure DNS.	Yes	Yes	Yes

Administering the dial rules on the application server

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **Dial Rules**.
2. Enter the appropriate information in the fields.
3. Click **Apply**.

Next steps

If your deployment has multiple application servers, administer a cluster.

Related links

Configuring a cluster on page 110
Dial Rules field descriptions on page 106

Dial Rules field descriptions

Name	Description
Dial Plan Handling	
Dial plan handling style	The options are: • Application server based: This is the Messaging Release 6.0 dial plan handling style, which is deprecated. This is the default option. • Site definition based: The site-based dial rules to perform dial rules tests and change the dial-out rules in the storage server.
Dial plan handling testing	The test that Messaging uses to verify and handle phone numbers correctly.
This Location	
Country code	The country code of the dialing phone number. Messaging uses the country code to determine if the calls are internal, local, domestic, or international calls. This field is deprecated. Use the **Country code** field on the Sites webpage.
Area code	The area code of the dialing phone number. For example, 212-5551212. Messaging uses the area code to determine if the outgoing calls are local or long distance calls. This field is deprecated. Use the **National destination code** field on the Sites webpage.
Dial-Out Settings	
Long-distance prefix	The digits preceding the area code of the dialing phone number. The default prefix is 1. This field is deprecated. Use the **National prefix** field on the Sites webpage.

Table continues…

Name	Description
International prefix	The digits preceding the country code of the dialing phone number. The default prefix is 011. This field is deprecated. Use the **International prefix** field on the Sites webpage.
Outside line prefix	The digits that users dial to gain access to an outside line. The default prefix is 9. This field is deprecated. Use the **Outside line prefix** field on the Sites webpage.
Company DID numbers that should be treated as internal numbers	
Number of digits in an extension	The length of the digits in an extension. If you are configuring: • **External (Public Network) Dial Plan Site**, configure the length of the digits required to call a number in the originating area code or a local call in the **Subscriber number length (within this site's national destination code)** field. • **Internal Dial Plan Site**, configure the length of the extensions of users on the site in the **Short extension length** field. This field is deprecated.
Number of DID ranges	The number of Direct Inward Dialing (DID) ranges for internal numbers. Messaging uses the DID range to route inbound calls to extensions within the range. This field is deprecated.
PBX Caller ID Information	
Caller ID internal number prefix	The dial-out prefix for internal calls. Messaging uses this field only when required by the telephony server for caller ID. This field is deprecated.
Advanced Rules	

Table continues…

Name	Description
Advanced Dial-out rules	The customized dial-out rules. Use the **Edit Dial-Out Rules** option 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 webpage to configure the dial-out rules.
Dial-in rules	The customized dial-in rules. The options are: • **system** • **custom** Customize the advanced dial-in rules only according to the instructions from Avaya Client Services.

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 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.

Table continues…

Name	Description
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	The script that 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. For new installations, Messaging does not block outgoing calls to emergency numbers. If you want the system to block outgoing calls to one or more emergency numbers, contact the Avaya Support center to have the dial-out rules script modified. If you have multiple sites on the same application server, use the same dial-out settings for emergency numbers.
Dial-Out Test Numbers	The option to define phone numbers to verify whether the Dial-Out Rules script handles these numbers correctly. You can also troubleshoot dial-out problems and verify that a given phone number is classified and dialed correctly. Define one phone number for each line as these phone numbers show like that in the directory or as users enter these phone numbers. For example, in the Mobile phone field, the Personal attendant field, the Reach Me settings, or the Notify Me settings.
Dial-Out Test Results	Information about the input phone number, the call type, and the output phone number. The call type can be internal, long distance, international, or invalid.
Dial-Out Script Configuration	Information about the dial-out script configuration . 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.

Configuring a cluster

About this task

You must add all 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 application server.

Repeat this procedures until you configure all application servers for your sites.

Before you begin

Define the application server as a member of the cluster.

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 increases to match the number that you entered.

3. In each **Member** field, enter the IPv4 or IPv6 address of an application server in the cluster. You can specify the IPv6 address for cluster member, if IPv6 is enabled on the application server.
   - For a new cluster member, add 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.
4. Click **Apply**.

   The system displays a confirmation message.

5. Click **OK**.

Next steps

Administer the fax feature to send and receive messages.

Related links

Fax administration checklist on page 112
Adding additional application servers on page 132

Cluster field descriptions

Name	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.

Fax administration checklist

Messaging supports sending and receiving fax. Use the following checklist to enable the fax feature for Messaging users.

For information about configuring Messaging to transfer fax calls to a fax server, see System Parameters field descriptions on page 178.

No	SMI page	Task	Topic	✔
1	—	Ensure that the telephony server uses the T.38 fax codec for fax calls.	—	
2	External Hosts	Administer the external SMTP host.	Administering the external SMTP host on page 76.	
3	Class of Service	Configure CoS for fax support.	Class of Service field descriptions on page 216.	
4	System Parameters	Configure the application server to send and receive fax.	Enabling fax on page 112.	
5	Class of Service	Enable the email notification that Messaging sends to users after Messaging successfully sends a fax.	Class of Service field descriptions on page 216.	
6	System Administration	Enable the encryption of fax transmissions between application servers.	System Administration field descriptions on page 159.	
7	System Administration	Administer the number of SIP sessions that Messaging supports for outbound faxes.	System Administration field descriptions on page 159.	
8	—	In User Preferences, specify the email address for Messaging to forward the fax.	—	

Enabling fax

About this task

If your deployment has multiple application servers, enable fax for each application server on the site.

For more information about the procedures that you must perform manually and the procedures that Messaging automatically performs through the backup and restore process, see *Initial administration checklist for application roles*.

Before you begin

If you are administering the first or the only application role, integrate the telephony server.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **System Parameters**.
2. Enter the appropriate information in the **Fax** area.
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, administer languages.
- If you are administering additional application servers that support the same site as the first server, restore the data of the first server on the other servers.
- Tell your users about installing the fax client. For more information, see *Using Avaya Aura® Messaging*.

Related links

Integrating with the telephony server on page 134
Configuring languages on page 115
Restoring application files on page 288
Initial administration checklist for application roles on page 105
System Parameters field descriptions on page 178

Messaging fax client on Windows

You can compose a document in a Windows-based program and fax it from your desktop to any fax destination. The Messaging fax client sends the document to the fax printer service on the Avaya message store. The fax printer service sends the document to the application role, which sends it to the fax destination. For new installations, Messaging supports silent installations of the outbound fax desktop client on Windows 8.1 and Windows 10.

Messaging supports installation of a fax client by using one of the following methods:

- Manual method
- Push method
- Silent method

Manual method

The Messaging users can install the fax client on their desktop. For more information, see *Using Avaya Aura® Messaging*.

If you select the manual method, inform the end users about the following prerequisites:

- Configuring Internet Printing Protocol (IPP) and HyperText Transfer Protocol (HTTP).
- Uninstalling the CallPilot® Desktop Messaging client before installing the Avaya Aura® Messaging Fax Client.

Push method

You can push the fax client installation using two methods:

- Group policy: Group policy supports two methods for deploying the fax client msi package:
  - **Assign software**: You can assign the program to each user or machine. When you assign the program to a user, then the software is installed when the user log on. When you assign the program to a machine, then the program is installed for all users when the machine starts.
  - **Publish software**: You can publish the software for one or more users. The user can install the program from the Add or remove programs list.
- SMS: You can edit the .sms (Systems Management Server) file and then create a package from the .sms file.

For more information, see the following Microsoft website :https://technet.microsoft.com/en-us/library/cc738858(v=ws.10).aspx.

Silent method

Use this method to do the automatic installation of the fax client for a large number of users. Installing the fax client automatically does not require user interaction and does not display messages or prompts. You can install the fax client by running a command on the command line interface.

Note:

A user with fax messaging capability must uninstall the CallPilot® Desktop Messaging client from the system before installing Avaya Aura® Messaging Fax client. Ensure that the CallPilot® fax printer driver is also uninstalled from the system. When you attempt to install the Avaya Aura® Messaging Fax client, the system displays a message: "`CallPilot Desktop Messaging is currently installed on your desktop. You must uninstall the program before you can install the Avaya Aura Messaging Fax Client.`"

Installing Fax client in silent mode on Windows

About this task

Use this procedure to download the fax client .msi file from the Messaging storage server and install it.

Procedure

1. Start the program from the **Start** menu.
2. In the **Run** window, type `cmd`.
3. On the command line interface, type the following: `msiexec /I FaxClient-en-US.msi /quiet`.

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.

Note:

Messaging supports bilingual system announcements for English-US and French-Canadian languages in a multi-language Avaya Multimedia Messaging deployment. To use this feature, you must install the bilingual language packs in conjunction with at least one other language pack. A bilingual language pack can only be used as a site default language.

Configuring languages

About this task

The default US English language pack in Messaging contains the standard prompts. The language pack that contains rapid prompts is optional and is only available in US English for the Aria TUI. The standard prompts contain more details than the rapid prompts. The shorter rapid prompts, which help users save time, are for the users who are familiar with the TUI capabilities.

If you set up the rapid prompts on Messaging, users can view the rapid prompts check box on the My Phone webpage in User Preferences.

The following system features use the languages that you select on the Languages webpage:

- User Preferences
- TUI
- Name playback
- TTY

Important:

- When you add a language pack, Messaging disconnects all active calls. Additionally, the Messaging system will be unavailable for some time.
- If your deployment includes more than one server in the application role, you must configure languages on each application server. For more information about the procedures that you must perform manually and the procedures that Messaging

automatically performs through the backup and the restore process, see *Initial administration checklist for application roles*.

- If you install more than three language packs on one application server, do not enable the speech recognition for the sites or the classes of service on the application server. If you enable the speech recognition, you might exhaust the memory capacity.

Note:

If you need support with language packs, contact Avaya Services.

Before you begin

If you are administering the first or the only application role, enable fax.

Procedure

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

   The system saves the language packs that you added.

Next steps

- If you are administering the first or the only application role for a site, change the AxC IP address.
- If you are administering additional application servers that support the same site as the first server, restore the application files from the first server.

Related links

Enabling fax on page 112
Loading lists on page 146
Administering the server role and AxC IP address on page 42
Restoring application files on page 288
Initial administration checklist for application roles on page 105
Languages field descriptions on page 117

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	
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 and upload the packs.
Delete Language Pack	Select and delete a language pack from the drop-down list of installed language packs. You cannot delete a language pack if the language: • Is selected by a local or remote user in User Preferences. • Is administered for a Messaging access number. • Is administered for Auto Attendant. • Is administered as **System Language** or **Default Subscribe UI Language** on the Languages webpage.

Deleting languages

About this task

If Messaging contains the maximum supported language packs, you can delete language packs to add new language packs.

Before you begin

Ensure that the language pack that you want to delete is not:

- Selected by a local or remote user in User Preferences.
- Administered for a Messaging access number.
- Administered for Auto Attendant.
- Administered as **System Language** or **Default Subscribe UI Language** on the Languages Web page.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **Languages**.
2. From the **Delete Language Pack** drop-down list in the **Language Packs** section, select a language.
3. Click **Delete**.

   Messaging deletes the language pack.

Verifying the status of the application role

About this task

The System Status webpage displays the status of the following processes and the AxC connection:

- Application software release
- System uptime
- AxC IP address
- Time
- Voice Messaging Application - Last known AxC status
- Voice Browser - Speech Server
- User Data Migration
- Application Distributed Cache Server
- Storage Synchronizer

- Messaging Web Access
  - Java Servlet Container (Tomcat)
  - HTTP Server (Apache)
  - Flash Policy Server

Note:

After you migrate data from another Messaging system, ensure that the **User Data Migration** process is in the *Not Running* state before restarting Messaging.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Information** > **System Status**.

   Messaging displays the results.

2. To view the updated results, click **Refresh**.

Chapter 6: Sites and topology

Initial administration checklist for sites and topology

Use the following checklist to administer the sites and topology of Messaging for the first time. In large organizations with specialized administration roles, the Messaging administrator usually performs these tasks.

No.	SMI page	Task	Location		✔
			Single-server systems	Front-end / Back-end systems	
1	Sites	Adding additional sites on page 126.	Single server	Storage server	
2	Sites	Assigning language menu choices for a site on page 127.	Single server	Storage server	
3	Topology	Activating sites on page 52.	Single server	Storage server	
4	Telephony Integration	Integrating with the telephony server on page 134.	Single server	Application server	
5	System Status	Verifying the status of the storage role on page 103. Verifying the status of the application role on page 118.	Single server	Storage server and application server	
6	System Operations	Verifying the link to AxC on page 146.	Single server	Application server	
7	System Operations	Loading lists on page 146.	Single server	Application server	

Initial site administration

Sites overview

A Messaging site is a set of properties that you define in the System Management Interface (SMI). Each Messaging system has at least one site, but each system can support 500 sites.

Each user can be a member of only one site. For single-site systems, Messaging automatically assigns all users to the default site. For multi-site systems, you must assign a site for each user. The system compiles each list of users into a system-wide directory that Auto Attendant uses for name dialing, addressing by speaking a name, and speech look up.

Sites with speech recognition

The system supports the following properties for sites with speech recognition:

- A site identifier that includes the extension style required by the telephony server, the country code, the site prefix. It may include the national prefix for countries that have a convention of prepending the national prefix for International dialing. For example, site identifier = **Country code** + **Site prefix** if '**International dialing (to this country)**' is set as '**Do not prepend National Prefix**' for the site and site identifier = **Country code** + **National prefix** + **Site prefix** if '**International dialing (to this country)**' is set as '**Prepend National Prefix**.
- Messaging access numbers, also called pilot numbers, for both internal and external callers.
- Universal addressing options. For example,
  - **Local**
  - **National**
  - **Global**
- Up to two customer-installed languages.

  Because all application servers in a cluster must have an identical set of languages, you must install the same languages onto clustered application servers. Then, for each site that the cluster supports, you must select a default language for the Messaging access number. You can also select two additional languages for each site.

  When you configure a site to use speech recognition, do not install more than two languages onto the application servers that host the site. If you exceed this limit, you might exhaust the memory capacity that speech recognition requires. You cannot delete U.S. English. If you need more than three languages (U.S. English plus two customer-installed languages), configure your system with multiple clusters.
- Auto Attendant features. You can add up to 10 Auto Attendants. Each Auto Attendant supports up to two additional languages.
- P-Asserted Identity information for enforcing network security policies.
- Telephony Profile Name of the far-end SIP domain.
- 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.
- Optional system greeting that Messaging plays before playing the user greeting. You can use the system greeting to play additional messages such as standard disclaimers.

Sites without speech recognition

The system supports the following properties for sites without speech recognition:

- A site identifier that includes the extension style required by the telephony server, the country code, the site prefix. It may include the national prefix for countries that have a convention of prepending the national prefix for International dialing. For example, site identifier = **Country code** + **Site prefix** if '**International dialing (to this country)**' is set as '**Do not prepend National Prefix**' for the site and site identifier = **Country code** + **National prefix** + **Site prefix** if '**International dialing (to this country)**' is set as '**Prepend National Prefix**'.
- Messaging access numbers, also called pilot numbers, for both internal and external callers.
- Universal addressing options. For example,
  - **Local**
  - **National**
  - **Global**
- Up to 15 customer-installed languages.

  Because all application servers in a cluster must have an identical set of languages, you must install the same languages onto clustered application servers. Then, for each site that the cluster supports, you must select a default language for the Messaging access number. You can also select two additional languages for each site.
- Auto Attendant features. You can add up to 10 Auto Attendants. Each Auto Attendant supports up to two additional languages.
- P-Asserted Identity information for enforcing network security policies.
- Telephony Profile Name of the far-end SIP domain.
- 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.
- Optional system greeting that Messaging plays before playing the user greeting. You can use the system greeting to play additional messages such as standard disclaimers.

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 AxC 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 **Synchronize** next to **Application Distribution Cache (ADCS)** on the System Operations Web page.

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 shorter in length, but are still uniquely identifiable in the global context.

E.164 is an ITU-T recommendation that defines the international public telecommunication numbering plan used in the PSTN and some other data networks. It also defines the format of telephone numbers. E.164 numbers can have a maximum of 15 digits and are usually written with a + prefix. To actually dial such numbers from a normal fixed line phone, the appropriate international call prefix must be used.

Dial rules

Dial plan overview

A Messaging dial plan defines how your Messaging system integrates with the telephony server (PBX) and categorizes user-defined telephone numbers according to call types. Administrators can define a short version of the voice mailbox and the telephone extension to enhance the user experience during login and message addressing.

If your Messaging system arrives with one default site, you must configure the site with dial plan information. Large enterprises with multiple sites must configure one dial plan for each site. If your Messaging system supports 500 sites and, therefore, you must configure 500 dial plans. And

when more than one site uses the same dial plan you can manually copy the dial plan to other sites.

The system stores dial plans on the storage server, which automatically applies them to the appropriate application server as defined in the Topology SMI.

Dial plan style

Messaging supports two dial plan styles:

- Application server based: The earliest versions of Messaging supported one site with one dial plan stored on the application server. Select this style only if you are upgrading from an earlier release and have no plans to add another site or to use the E.164 numbering plan. All other customers must select the site-based dial plan.
- Site definition based: To support multiple sites, Avaya moved the dial plans to the storage server, which then applies each plan to the appropriate application server. Select this style to install a new system, even a single-site system. Also select this style to expand the number of sites or integrate with Avaya Aura® Session Manager.

  If you want to move from a server-based system to a site-based system, you must manually reenter dial plan information. No automated tool is available for migrating dial plan data between plan styles.

Migrate your dial plan data

If you upgrade Messaging Release 6.0.1 and use application-based dial rules, you must manually move the data from the Dial Rules webpage, Dial-Out Rules Script, and the Attendant/Operator webpage to the Sites webpage.

Perform the following:

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

The following table includes information about the fields that you must use after the upgrade:

Dial Rules webpage (Preupgrade)	Sites webpage (Post upgrade)	Comments
Country code	Country code	The country code of the dialing phone number.
Area code / Private number	National destination code	The sequence of digits at the beginning that the telephony server considers local other than the one defined for the telephony server.
Long-distance prefix	National prefix	The digits before the area code of the phone number.

Table continues…

Dial Rules webpage (Preupgrade)	Sites webpage (Post upgrade)	Comments
International prefix	International prefix	The digits before the country code of the phone number.
Outside line prefix	Outside line prefix	The digits required to access the outside line.
Number of digits in an extension	Subscriber number length (within the national destination code of this site) and Short extension length	If you are configuring an: • External dial plan, set the length of the digits required to call a local number in **Site External (Public Network) Dial Plan Site** > **Subscriber number length (within this site's national destination code)**. • Internal dial plan, set the length of the digits required to call the extensions of users within a site or an enterprise location in **Site Internal Dial Plan** > **Short extension length**.
Number of DID ranges	—	This field is removed.
Caller ID Internal Number Prefix	—	This field is removed.
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 webpage (Preupgrade)	Sites webpage (Post upgrade)	Comments
Schedule type	Availability	The availability of the attendant.
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 if the attendant is unavailable.

Defining dial rules

Use dial rules for the following features:

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

- Outbound Fax

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**
3. Click **Save**.

Next steps

- Configure the attendant for a site.

Related links

Assigning an attendant number on page 128
Sites field descriptions on page 53

Adding additional sites

About this task

Depending on your deployment requirements, add additional sites. If you do not need to add more sites, define your system topology.

Complete the following instructions on the storage server. Restart Messaging after you add more sites.

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.
4. Click **Save**.
5. Restart Messaging.

Next steps

Define your system topology.

Related links

Stopping Messaging on page 460
Starting Messaging on page 460
Overview for administering topology on page 130
Sites field descriptions on page 53

Deleting a site

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Sites**.
2. In the **Sites** section, in the **Sites** field, click the site that you want to delete.
3. Click **Delete**.

   The system displays a confirmation message.
4. Click **OK**.

   When you attempt to delete a site to which users, info mailboxes, and caller applications are associated, the system displays a message such as "`Site cannot be deleted because it is assigned to one or more users, info mailboxes or caller applications.`"

   Rectify the conditions that prevent you from deleting a site and try to delete the site again.

Assigning language menu choices for a site

About this task

Install language packs on application servers, and create sites on a storage server. Use this procedure to create language menu choices for a site.

Before you begin

If you upgrade Messaging, you must install the language packs again.

Procedure

1. Define a new site using the Sites webpage.

   The default language of each site is English-US, which is also the default system language. Other language menu choices are available only after you map sites and application servers.
2. Create the site-application server mapping using the Topology webpage.
3. To select a language from the available languages installed on the mapped application server, update the site that you created in Step 1 using the Sites webpage.
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 webpage to select the language pack.
5. If you change the default site language, reload User List and Global Address List.

Related links

Configuring languages on page 115

Adding additional application servers on page 132
Loading lists on page 146
Setting the site properties for the first time on page 50

Assigning an attendant number

About this task

When a caller presses 0 to reach an attendant, the system transfers the call to the assigned extension. If the attendant does not answer, the system transfers the call to a general delivery mailbox so that the caller can leave a message. The caller leaves a message only if you administered a mailbox in **General mailbox** on the Sites page.

The system preserves the language selection of the caller in the Auto Attendant menu when the system changes the call into a covered call, that is, a Ring-No-Answer scenario. The system does not save the information if:

- The system covers the call at another application server where you did not install the corresponding language pack.
- You did not install Communication Manager Release 6.2 and later.

The system presents the language menu to the caller at Auto Attendant. You can configure up to 10 Auto Attendant pilot numbers for each site. Each Auto Attendant number supports up to three languages.

Important:

If you enable speech recognition for a site, ensure that the application server that hosts the site does not have more than three language packs installed. If you exceed this limit, you might exhaust the memory capacity.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Sites**.
2. In the **Operator (Live Attendant)** section, in the **Availability** field, select one of the following:
   - **Never**: Messaging transfers the caller to the mailbox that you administer in **General mailbox**. This option is the default option.
   - **Always**: Messaging transfers the caller to the extension that you administer in **Operator (live attendant) extension**.
3. In the **Operator (live attendant) extension** field, type the extension of the attendant.

   SMI activates the **Operator (live attendant) extension** field only if you select **Always** in the **Availability** field.

   If you select **Always** in Step 2 and do not enter an extension number, SMI does not let you save the changes.
4. In the **General mailbox** field, type the shared mailbox number that is accessible to all attendants.

SMI activates the **General mailbox** field only if you select **Never** in the **Availability** field.

If you do not administer an extension number in **Operator (live attendant) extension** and a mailbox number in **General mailbox**, Messaging informs the caller that no one is available to attend to the caller and transfers the caller back to Auto Attendant.

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

   You can configure up to 10 Auto Attendant pilot numbers for each site. Each Auto Attendant number supports up to three languages.
7. In the **Default Language** field, click the language that you want as the default for the Auto Attendant number. You can select two additional languages for the Auto Attendant number.
8. Click **Save**.
9. Restart Messaging.

Next steps

Change the default greetings.

Related links

[Stopping Messaging](#) on page 460
[Starting Messaging](#) on page 460
[Changing Auto Attendant greetings](#) on page 129

Changing Auto Attendant greetings

About this task

You can upload the `.wav` files to Messaging and change the default greetings in Auto Attendant to your customized greetings.

Note:

If you change the default greetings, you can revert the customized greetings to the default greetings using **Restore Default** button.

Before you begin

Ensure that you:

- Add a site. The Auto Attendant settings are unavailable when you are adding a site.
- Have audio prompts of the customized greetings to upload to Auto Attendant in the `.wav` format.

  Important:

  You must use the 8,000 Hz/8-bit mono u-law format. If you use other formats, Messaging might experience issues when playing greetings.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Sites** and scroll to the **Auto Attendant Greeting / Menu** section.
2. In the **Inital Greeting** field, to select the `.wav` file of your customized initial greeting, click **Browse**.
3. Select the file and click **Open**.
4. Click **Upload (Replace Current)** to upload the `.wav` file and change the default initial greeting.
5. To select the `.wav` file of your customized **Menu** greeting, perform one of the following tasks:
   - Click **Browse** for the **Menu (keypad entry is basic)** field, and select the `.wav` file of the customized greeting to play when **Speech recognition** in Auto Attendant is *disabled*.
   - Click **Browse** for the **Menu (keypad entry is enhanced)** field, and select the `.wav` file of the customized greeting to play when **Speech recognition** in Auto Attendant is *enabled*.
   - Click **Browse** for the **System greeting before call answering** field, and select the `.wav` file of the customized greeting to play before a call is answered.

Related links

Recording and sending audio prompts on page 269
Getting audio prompts using Microsoft Outlook on page 269
Adding additional sites on page 126

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.

Mutare Message Mirror™

Messaging interoperates with Message Mirror to achieve a complete disaster recovery of voice messages and related information such as 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
- LDAP changes to a backup message store

Adding additional application servers

About this task

Use this procedure to:

- Restart Messaging after you add application servers.
- 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.
- Add the first application server to the site.
- 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.
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.

Next steps

Configure a cluster of application servers.

Related links

Adding the first application server on page 51
Stopping Messaging on page 460
Starting Messaging on page 460
Configuring a cluster on page 110
Initial administration checklist for application roles on page 105

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 corresponding parameters on the telephony server.

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

Telephony parameters

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

- Call Control PHB and Audio PHB. This information is only required if your IP network infrastructure supports the QoS features.
- The transport method of the far-end connection that you want to integrate.
- The IP address and the port number of each far-end connection or SIP proxy server.
- The names of the Messaging SIP domain and the far-end domain for each telephony profile that you want to create.
- The number of messaging trunks.
- (Optional) The type of 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 IP address.

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

About this task

If your deployment includes more than one application server, perform these steps on each application server.

Before you begin

- Add telephony domains on the Telephony Domains page.
- Gather information about the telephony server parameters that you need for integration.

Procedure

1. On the **Administration** menu, click **Messaging** > **Telephony Settings** > **Telephony Integration**.
2. Enter the appropriate information in the fields.
3. Click **Save**.

   Messaging prompts you to choose if you want to restart immediately or wait for all calls to finish and restart later.
4. To restart the telephony processes, click:
   - **Restart Immediate** to restart the telephony processes immediately.
   - **Restart Camp-on** to wait for all calls to end and restart the telephony processes.

5. **(Optional)** If Messaging displays the `Telephony processes failed to restart` message, restart Messaging.
6. **(Optional)** If Messaging displays the `WARNING: Failed to write config file. Restart aborted.`, restart the telephony processes again.

   If the telephony processes still fail to restart, restart Messaging.
7. If you changed any of the following switch link parameters, restart the telephony processes:
   - **Switch Integration Type**
   - **Messaging Ports**
   - **Switch Trunks**

Next steps

- Validate the Messaging telephony integration.
- Enable fax if required.
- Administer another application role if required.

Related links

Adding telephony domains on page 48
Stopping Messaging on page 460
Starting Messaging on page 460
Enabling fax on page 112
Restoring application files on page 288
Integration requirements on page 133
Telephony Integration field descriptions on page 91
Telephony Integration checklist on page 143

Telephony Integration field descriptions

BASIC CONFIGURATION

Name	Description
Switch Integration Type	The type of switch integration that Messaging uses. The SIP SPECIFIC CONFIGURATION section is available only for SIP integration.

SIP SPECIFIC CONFIGURATION

SMI displays the following section only if you click **SIP** in the **Switch Integration Type** field. On the Telephony Integration page, you have read-only access to these fields. You can administer these fields on the Telephone Domains page.

Name	Description
Far-end Domains	The number of far-end SIP domains. SMI displays the number of rows that are equal to the number of far-end SIP domains that you select from the drop-down list. You can add maximum 500 SIP domains.
SIP Domain	The domain names of the application server and the far-end connection. For example, sip.example.com. • **Telephony Profile Name**: The name of the telephony profile that represents a gateway ID and SIP domain of the application server. • **Gateway ID**: The ID of the far-end connection gateway. • **Messaging SIP domain**: The name of the Messaging SIP domain. • **Far-end domain**: The name of the far-end SIP domain connection.
Far-end Connections	The number of connections to the far-end SIP proxy servers. SMI displays the number of rows that are equal to the number of far-end SIP domains that you select from the drop-down list. You can add maximum 25 far-end connections.
Connection	The connection details of a far-end connection that includes: • **Gateway ID**: The ID of the far-end connection gateway. • **IP**: The IP address of the connection. • **TCP or TLS**: The transport method that the telephony server uses for SIP signaling. The transport method of the application server and the telephony server must match. The types of transport methods are: - **TCP**: Not encrypted. - **TLS**: Encrypted. • **Port**: - **TCP**: 5060 - **TLS**: 5061 • **Monitor interval**

Table continues…

Name	Description
Messaging IPv4 Address	The address of the near-end application server. This address is always a read-only field. • **IP**: Use the IP address of the server. • **TCP Port**: Use port 5060. • **TLS Port**: Use port 5061.
Messaging Ports	The maximum number of active calls to or from a user. • **Call Answer Ports**: The range of the ports, which is from 2 to 100. • **Maximum**: The maximum number of ports that Messaging uses. • **Transfer Ports**: The maximum number of transfer ports that Messaging uses.
Switch Trunks	The number of trunk members for Messaging on the telephony server. • **Total**: The total number of trunks administered. Messaging requires at least one more port than the number of ports that you administer in **Call Answer Ports**. • **Maximum**: The telephony server supports maximum 120 trunk members. The trunk members, in addition to the call answer ports, are for features such as the transfer feature, which require more switch trunks. If the telephony server specifies the maximum number of trunks, the number in the **Switch Trunks** field must match the number on the telephony server.

ADVANCED OPTIONS

When the ADVANCED OPTIONS section is hidden, SMI displays the **Show Advanced Options** button. When you click **Show Advanced Options**, the button changes to **Hide Advanced Options** and SMI displays the ADVANCED OPTIONS fields.

Name	Description
Quality Of Service	The QoS field to administer: • **Call Control PHB**: The quality of service level for call control messages. • **Audio PHB**: The quality of audio streams. Use this field if your IP network infrastructure supports QoS. You can keep the default values in QoS or enter new values. The values you enter must match the number in the network region of the telephony server. This is the telephony server that the Messaging signaling group uses. The range for both these fields is 0 to 63.
UDP Port Range	The range of port numbers used by UDP for RTP. The default range is 8000 to 10000. • You can change the **Start** value. • Messaging 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 the ports used for other purposes.
G.729 Codec Support	The option to enable support for the G.729 codec for media transmission. • If you select this check box, Messaging supports the G.729 and G.729A codecs with the G.711 μ-law and G.711 A-law codecs. • If you clear this check box, Messaging only supports the G.711 μ-law and G.711 A-law codecs. **Note:** Messaging supports the G.711 and G.729 codecs only for media transmission. Messaging supports the GSM codec and the G.711 codec for storage encoding.
Minimum TLS Version	The minimum TLS version that the telephony server uses for SIP signaling on the TLS port. The default TLS version is 1.0. Ensure that all far-end SIP proxy servers support the selected TLS version or higher.

Table continues…

Name	Description
Media Encryption	The type of SRTP media encryption that the telephony server uses. This field is optional. **Note:** The storage server must be online for the media encryption-related changes to take effect. If you have a single-server installation, Messaging must be running.
Enforce SIPS URI for SRTP	The option to specify whether a SIPS URI or secure URI is required for SRTP. If you set the value to **yes**, then any incoming call that contains SRTP without a SIPS URI fails.
SIP INFO for DTMF	The SIP INFO messages for the out-of-band DTMF. The options are: • **Ignore**: Ignore all SIP INFO DTMF digits in the signaling stream. This is the default value. • **Accept**: 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 milliseconds.
Include “AAM” in From/P-AI Header	The option to add “AAM” in the From SIP header and P-Asserted Identity SIP header.
Media Encryption During CapNeg	The SRTP media encryption that the telephony server uses when capability negotiation (CapNeg) is present in SDP. The options are: • **Enabled**: Set the default value. • **Disabled**: Change the value in the **Media Encryption** field to **None**. Messaging automatically changes the value, and you cannot change the value. Select **Disabled** only for a specific telephony integration. For more information about administering the media encryption during CapNeg, see the configuration notes.

Table continues…

Name	Description
Supported Header includes “replaces”	The supported header that must include the *replaced* value so that endpoints reflect the capabilities in SIP headers and Messaging effectively communicates with a specific telephony integration. The options are: • **no**: The default value. • **yes**: Only for a specific telephony integration. For more information about administering the header with the *replaces* value, see the configuration notes.
Telephone Event Payload Type	The RTP payload type for RFC2388 DTMF events. The dynamic payload type range is *96* to *127*. The default value is *127*. For example, when Messaging starts a call for a Reach Me operation, Messaging specifies the *127* RTP payload type for RFC2388 DTMF events. This field is inactive if you set the SIP INFO for DTMF field to *Accept*.
Monitor Far-end OPTIONS messages	The option to enable Messaging to proactively monitor the SIP OPTIONS messages that the far-end connection sends. If Messaging does not receive a SIP OPTIONS message from the far-end within the time specified in the **Proactive Interval** field, Messaging considers the far-end as nonfunctional or unreachable. The options are: • **no**: Disables monitoring of the OPTIONS messages. This is the default value. • **yes**: Enables monitoring of the OPTIONS messages. • **Proactive Interval**: The interval, in seconds, for which the far-end is configured for sending the OPTIONS message.

Table continues…

Name	Description
Inactive Link Actions	The option to generate an alarm or disconnect all incoming connections. The options are: • **Alarm Only**: Messaging generates an alarm when an expected OPTIONS message does not arrive within the interval configured in **Proactive Interval** + 30% of the interval period. For example, if you configure the interval as 10 seconds, Messaging generates an alarm after 10 + 3 (30% of 10) = 13 seconds. On the next successful receipt of SIP OPTIONS or the next incoming call, Messaging clears the alarm. • **Close Connections**: Messaging generates an alarm, closes all incoming connections, and drops all active calls. This option is only available if you set the value of **Monitor Far-end OPTIONS messages** to **yes**.
Minimum Session Refresh Interval	The minimum session refresh interval in seconds. Usually, the refresh interval value is set to match the interval value administered for the switch.
SIP REFER Delay	The delay of the transfer operation in milliseconds when a Messaging outbound call is answered and the SIP REFER request sent. The value range is 0 to 5000 milliseconds.
Minimum Fax Power Threshold	The minimum power level threshold to detect the incoming CNG fax tone. The value range is 14000 to 1400000. The default value is 140000.

Table continues…

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: • P-Asserted Identity • Multiple SIP domains • SIP UUI
Cross-Switch Transfer	The option to enable and disable call transfers between different gateways. Cross-switch transfer is enabled by default.
Connection Audits	The option to enable the audit of the incoming, the outgoing, and the MWI SIP connections. By default, Messaging disconnects the connections that are idle for 30 minutes.
Customize Blocked Caller-ID	The option to customize the appearance of the blocked caller ID with a customized caller ID. This check box is clear by default. **Important:** To determine how the system displays the customized caller ID, check with your service provider. You can understand how the network of the service provider processes a blocked caller ID.

Table continues…

Name	Description
Blocked Caller-ID	The option to administer values to at least one of the following fields to customize the caller ID appearance: • **Username** • **Display Name** These fields are available if you select the **Customize Blocked Caller-ID** check box. • The user name and the display name: anonymous@anonymous.invalid • Only the user name: anonymous@anonymous.invalid • The user name with the SIP domain: anonymous-sip.com
Blocked Caller-ID Matches	The option to administer the SIP headers that Messaging examines to determine whether the caller ID of the incoming call is blocked. The options are: • **From Header**: To administer Messaging to examine the From SIP header. • **P-AI Header**: To administer Messaging to examine the P-Asserted Identity SIP header.

Related links

Support for SIP INFO messages on SIP connections on page 133

Telephony Integration checklist

Use this checklist to validate the Messaging telephony integration.

Before you begin validating the telephony integration:

- Configure the Pilot number on the telephony server.
- Complete the administration of all Messaging and other components, such as Session Manager, the AudioCodes media gateway, and PBX.

Check	Steps	Result/validate
Inbound calling	Call an extension and ensure that the system establishes the call to the application server.	When Messaging transfers a call to the voice mail, you must hear the ring tone and the system main menu. This result validates the call coverage function.

Table continues…

Check	Steps	Result/validate
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**.	Test a call to an: • Extension: Verify that Messaging connects the call to the extension. • Outside number: Verify that Messaging connects the call to the outside number. Ensure that the call stays connected for at least 60 seconds. This result validates the outbound calling to internal and external numbers.

Related links

Running application server diagnostics on page 422

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**.

   Messaging displays a confirmation message.
4. Click **OK** to proceed.
5. Restart Messaging.

Related links

Stopping Messaging on page 460
Starting Messaging on page 460

Topology field descriptions

Name	Description
Sites / Application Servers	The field that displays information about the sites that you created on the Sites webpage: • 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**: To add the first application server to a site. You can also add other application servers without administering a cluster. • **The same site configuration as an existing application server**: To add another application server to a 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 that is associated with the site. Ensure that you cluster the additional server with the existing ones.
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: • **Primary** • **Backup**

Verifying the link to AxC

About this task

After you configure the sites and topology, verify that the AxC connector can connect to each application server in your topology. You can test the connection by reloading User List and Global Address List.

If you have a multiserver configuration, complete this test on each application server.

Before you begin

Complete the steps listed in *Initial administration checklist for sites and topology*.

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 correctly connects the application role to AxC and the storage role. If the system returns an error message, verify that:
   - The IP address of AxC is correct.
   - The topology configuration is correct.
3. **(Optional)** Repeat Step 1 and Step 2 to ensure that the caches reload without error.

Related links

Administering the server role and AxC IP address on page 42
Overview for administering topology on page 130
Initial administration checklist for sites and topology on page 120

Loading lists

About this task

Use the System Operations webpage to load the following lists:

- User List
- Global Address List

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.

   The system displays the Operation in progress dialog box. When the system completes the reload operation, the dialog box does not show.

Messaging configuration checklist

Use this checklist as guidelines to validate the Messaging configuration. By doing these tasks, you can check the connection to the gateway and Exchange Server.

Before you validate the Messaging installation and configuration, do the following:

- Complete the installation and configuration of the Messaging system.
- Install the Microsoft Outlook form using Exchange Server.
- Configure Microsoft Outlook for each test user for IMAP access.

No.	Tasks	Reference	Note
1	Check whether all services are running	Verify the system status.	All required services are running.
2	Create test users	Add the following test users: • Create Test User1 with the *Standard* CoS setting. • Create Test User2 with the *Enhanced* CoS setting.	To check whether the system creates the test users, click **Messaging** > **Reports (Storage)** > **Users**.

Table continues…

No.	Tasks	Reference	Note
3	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 entering the email addresses. You can enter upto five email addresses, separated with a semicolon (;). Messaging supports only email based (SMTP) pager and cellular notifications. For more information, see *Using Avaya Aura® Messaging*.	—

Table continues…

No.	Tasks	Reference	Note
		Open User Preferences for Test User2 and set the following: • Select the General page and type a valid mobile number in the *Mobile Phone or Pager* area. • Select the Notify Me page and enable **Phone Notifications** using the number that you configured in the General page. • Select the Reach Me page and enable and configure three Reach Me numbers that consist of an internal extension and an external number. Messaging supports only email based (SMTP) pager and cellular notifications. For more information, see *Using Avaya Aura® Messaging*.	—
4	User initialization	As Test User1, do the following: • Call the Pilot Main Number from a phone that is registered to the extension assigned to the user. Ensure that this call is online for at least 60 seconds. • Provide temporary password according to the system prompts. • Change password. • Record spoken name. • Record greeting. • Hang up. 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. On 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. On entering your Mailbox and Password, the system guides you through the steps to initialize your mailbox.

Table continues…

No.	Tasks	Reference	Note
		As Test User2, do the following: • Call the Pilot Main Number from a phone that is not registered to the extension assigned to the user. • Press the pound key (#) to log in according to the system prompts and provide the mailbox number. • Provide temporary password according to the system prompts. • Change password. • Record spoken name. • Record greeting. • Hang up. For more information, see the *Using Avaya Aura® Messaging* guide.	This test validates: • Users are loaded appropriately on the Messaging server. • Integrated login. • Long duration outbound calls through any SBCs or gateways.

Table continues…

No.	Tasks	Reference	Note
5	Basic call answer	Do 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 the user details and the date and time when the message is sent. • Hang up. • From an outside number, dial the external Pilot number and enter Test User1 extension. • Leave a message. Note the external number and the date and time when the message is sent. • Hang up. For more information, see *Using Avaya Aura® Messaging*.	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 test validates: • Basic Call Answering. • Basic MWI functionality. • Email notifications. • Text message notifications. • Subject line matching.
6	Basic messaging	Do the following: • From extension of Test User1, call main pilot number. • Provide password to login according to the system prompts. • Listen to both messages. Do not delete the messages. • Observe that MWI turns off. For more information, see *Using Avaya Aura® Messaging*.	Observe the following: • Test User1 has two messages in inbox with appropriate time. • MWI updates to Off for Test User1. This test validates: • Capability to get messages using TUI. • MWI updates. • Subject line matching.

Table continues…

No.	Tasks	Reference	Note
7	Outcall notification. Skip this task if you do not use this feature.	Do the following: • Configure Enhanced CoS to enable Outcalling notification. In the **Class of Service** field, click the *Enhanced* COS from the drop-down list. Set **Allow outcalling notification** to *Yes*. 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 log in according to the system prompts. • Create a voice message for Test User2. Note the user details and the date and time message is sent. • Address the outcall for future delivery in n minutes. • Verify that outcall is started after n+5 minutes. Ensure that this call is online for at least 60 seconds. • Reset the **Start after** value to real system value. For more information, see *Using Avaya Aura® Messaging*.	Observe the following: • The system does not deliver the message until expected date and time. • Date and time stamp of message is according to the expected future delivery date. • Outcall notification occurs according to the schedule setting and only after the system delivers the message. This test validates: • System date and time is correct. • Outcall Notification. • Long duration outbound calls through any SBCs or gateways.

Table continues…

No.	Tasks	Reference	Note
8	Using Outlook toolbar. Skip this task if you do not 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 *Using Avaya Aura® Messaging*.	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 the correct date and time and the subject line information. • Online Help for toolbar is accessible. • User Preferences is accessible. This test validates: • Most Microsoft Outlook form actions. • Subject line matching. • Access to online help. • DNS for User Preferences is correctly set.
9	Reach Me Skip this task if you do not use this feature.	Do 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 caller can leave a voice message. This test validates the Basic Reach Me functionality for both types of phone numbers.

Table continues…

No.	Tasks	Reference	Note
10	AA call transfer to user. Skip this task if you do not use this feature.	Do 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 test validates: • Users are loaded appropriately on the application server. • Basic Auto Attendant functionality. • Speech addressing, if enabled. • Reach Me using Auto Attendant.

Related links

Changing a Class of Service on page 214
Changing user properties on page 191
Adding users on page 189
Verifying the status of the application role on page 118
Verifying the status of the storage role on page 103

Chapter 7: Managing servers

Storage servers

Message recording

Maximum Message Length on the System Mailboxes webpage defines the maximum length of a message, in minutes or MB, that a user can create in Messaging. This maximum length is a systemwide setting that applies to all users. You cannot change the maximum message length. However, you can set additional restrictions for users on the Class of Service webpage.

Use **Maximum voice mail message length** and **Maximum call answer message length** on the Class of Service webpage to define the maximum time for a message recording.

Adding a trusted server

About this task

Use the Add Trusted Server webpage to add trusted servers to the Messaging network. The servers might include:

- System Manager server
- Provision server
- Unimax 2nd Nature server
- Mutare Message Mirror server
- Avaya Site Administration(ASA) server
- 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 webpage, click **Add a New Trusted Server**.
3. On the Add Trusted Server webpage, in the **Special Type** field, click the type of trusted server.

If you select a common type of trusted server, the system automatically populates some of the fields on the **Add Trusted Server** webpage.

4. Enter the appropriate information in the fields.
5. Click **Save**.
6. To view a summary of the administered trusted servers on the Trusted Servers webpage, click **Display Report of Trusted Servers**.

Related links

Add Trusted Server field descriptions on page 156

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 that can include up to 25 characters and must not 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. You must specify a password that contains up to 10 alphanumeric characters.
Confirm Password	The field to 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 webpage. • 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** field.

Table continues…

Name	Description
Minutes of Inactivity Before Alarm	The number of minutes that 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.
Default Community	The default community number for the trusted server.
Access to Cross Domain Delivery	The option to allow cross-domain delivery through this trusted server.
Special Type	The type of trusted server. The system automatically populates or restricts some fields on the page based on your selection.
LDAP Access Allowed	The option to specify 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. The options are: • **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 setting is the default value.
IMAP4 Super User Access Allowed	The option to specify 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. The options are: • **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 setting 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 Administration**.
2. Enter the appropriate information in the fields.
3. Click **Save**.

Related links

System Administration field descriptions on page 159

Privacy enforcement

Messaging enforces the following levels of privacy when IMAP4 clients retrieve messages:

- 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.
  - Retrieves messages for clients who accept voice mail privacy.
  - 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 keeps the message private. Recipients must enforce the privacy of the message. Messaging cannot enforce privacy rules onto clients who cannot mark messages as private. Most clients do not restrict the forwarding of private messages. However, IMAP4 clients retrieve the .wav attachment of a private message.

You cannot use the System Administration webpage to make the following changes when you use a third-party message store such as Exchange:

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

Setting the privacy enforcement level for IMAP4 clients

Procedure

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

System Administration field descriptions

Administer the system features and the ports used by the Messaging storage server.

LOG-IN PARAMETERS

Name	Description
Login Retries	The number of times that a user can enter an incorrect password before Messaging cancels the login attempt. This field is read-only. The default value is 3 attempts.
Consecutive Invalid Attempts	The number of failed login attempts before Messaging locks the user account. The range is from 0 to 999. The default value is 18.
Minimum PIN Length	The minimum number of characters required for a password. The range is from 1 to 15. The default value is 7.
PIN History	The number of passwords that Messaging stores in history. Users cannot reuse these passwords when changing the mailbox password. For example, if you administer the value as 5, subscribers cannot use the last five passwords. If you set the value to 0, passwords are not stored in history.
Subscriber's PIN May Consist of a Single Repeated Digit	The option to set a password that contains a single repeated digit. For example, 1111.
Subscriber's PIN May Consist Solely of Consecutively Ascending Digits	The option to set a password that contains sequential digits in an increasing order. For example, 1234.
Subscriber's PIN May Consist Solely of Consecutively Descending Digits	The option to set a password that contains sequential digits in a decreasing order. For example, 4321.

Table continues…

Name	Description
Subscriber's PIN May Match Mailbox Number	The option to set a password that can be identical to the mailbox number.
Subscriber's PIN May Be a Subset of Mailbox Number	The option to set a password that can be a subset of the mailbox number.
Subscriber's PIN May Be a Subset of Reverse of Mailbox Number	The option to set a password that can be a subset of the reverse of the mailbox number.
Subscriber's PIN May Match Reverse of Mailbox Number	The option to set a password that is identical to the sequential reverse of the mailbox number.
Subscriber's PIN May Contain Mailbox Number	The option to set a password that contains the mailbox number.
Subscriber PIN May Contain Reverse of Mailbox Number	The option to set a password that contains the sequential reverse of the mailbox number.
Lock Duration	The time duration (number of minutes) for which a mailbox account is locked after a user fails to login before unlocking automatically. The default value is 10800 minutes (One week). The valid values are 0, 5–43200. When you upgrade Messaging from 6.2.5 to 7.1.0, then the default value in the **Lock Duration** field must be 30 minutes. If there is no setting for **Lock Duration** in Messaging 6.2.5, then ensure that after upgrading to Messaging 7.1.0, the default value is not 0.
Lockout Notification Mailbox	The mailbox number, where a locked login notification is sent. When a local mailbox gets locked, Messaging sends out a notification message to the **Lockout Notification Mailbox** number.

SUBSCRIBER PIN AGING LIMITS (DAYS)

Name	Description
PIN Expiration Interval	The number of days after which the password expires. • The valid values are from 0 to 999. • The default value is 0. This field is relevant only when you enable Password Aging on the Class of Service webpage.
Minimum Age Before Changes	The minimum number of days after which you can change the password.

Table continues…

Name	Description
Expiration Warning	The number of days that must pass before users can change their passwords again after a successful change. • The valid values are from 0 to 999. • The default value is 0 If users do not change passwords within a specified time, the password expires and Messaging blocks the user until an administrator resets the password.

MISCELLANEOUS PARAMETERS

Name	Description
System Prime Time, Start	The start time, in hours and minutes, of the prime time interval. The start time is usually the time that your company is open for business. The default is 08:00.
System Prime Time, End	The end time, in hours and minutes, of the prime time interval. The end time 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 are available in the system during a full remote update. When the system reaches the maximum limit, you cannot request a full remote update until one of the sessions is finished. The default is 100. The range is 0 to 100.

Table continues…

Name	Description
Anonymous LDAP Authentication	The option using which trusted LDAP clients can authenticate and connect to the LDAP database, or unauthenticated clients can anonymously connect to the database. • **Authenticated Only**: To give access to trusted LDAP clients to authenticate and connect to the LDAP database. Connection to the database as a trusted server requires the name of the trusted server, the IP address, and the password that matches the details of the server administered on the **Trusted Servers** webpage. Trusted servers can get and change LDAP data. Authenticated subscribers can get a subset of the subscriber information in the database, such as the email address and the extension number. • **Authenticated or Anonymous**: To give access to unauthenticated LDAP clients to connect to the LDAP database. Unauthenticated clients can get a subset of the subscriber information in the database, such as the email address and the extension number. For example, email clients can anonymously connect to the LDAP database to access the subscriber data.
Maximum Recorded Name Time (sec)	The maximum duration of time in seconds for recording a name. The values range from 1 through 20. The default value is 10.
Default Internet Subscriber Community	The default community assigned to subscribers external to the system. These internet subscribers include all email addresses not known by the system as local or remote subscribers.

FEATURE ACTIVATION

Name	Description
Privacy Enforcement Level	The option to assure privacy. 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 Server, the privacy enforcement level must be *Email*.
Automatic Mail Forwarding	The option to forward mail automatically. For Exchange Server, the value must be *yes*.

Table continues…

Name	Description
Allow email Notification for Private Messages	The option that administrators use to send private messages as email notifications to a subscriber mailbox. This setting is relevant if you enable **Allow email notification** on the Class of Service webpage for one or more users. The options are: • **Yes, with or without recording** • **Yes, only without recording** • **No** If you enable this option, users receive email notifications depending on the Notify Me settings on their personal User Preferences. Messaging delivers email notifications in the `.wav` file format.
Login Announcements May Not Be Skipped by User	The option to enforce the user to listen to the complete login announcement on the first login.
Login Announcements are Played Every Time a User Logs In	The option using which you restrict the user from deleting the login announcement.
Maximum SIP Sessions for Outgoing FAX (per Application Server)	The option to administer the maximum number of SIP sessions for outbound fax. The valid values are 1 to 20. The default value is 1.
Use SSL When Relaying Faxes Between Application Servers	The option to encrypt faxes between application servers. When you select this check box, SSL encrypts the connection between the application servers and the storage servers. If the application server and the storage server are coresident, this option is not required.
Transfer Domain Policy	The SIP domain that Messaging uses for call transfer operations such as Auto Attendant, Personal Operator, Call Sender, and Transfer to Extension. The options are: • **Subscriber's Domain**: Administer Messaging to use the SIP domain of the subscriber to transfer a call. When a subscriber is not associated with the call, such as calls to Auto Attendant, Messaging uses the SIP domain of the site where you administer the Auto Attendant number. • **Calling Party's Domain**: Administer Messaging to use the SIP domain of the caller to transfer a call. This option is the default setting. A call might fail if the Call Sender feature starts an outbound call to a user who administers a different SIP domain than the SIP domain administered in Messaging. This call failure depends on the path of the transferred call established between the SIP networking components.

Table continues…

Name	Description
Notify Me By Email 'From:' Address	The email address that the **Notify-Me By Email** feature inserts into the From: field. If this field is blank, then Messaging inserts the email address of the user who receives the message triggering the notification.
Notify Me By Text 'From:' Address	The email address that the **Notify-Me By Text** feature inserts into the From: field. If this field is blank, then Messaging inserts the email address of the user who receives the message triggering the notification.
Generate TNEF Attachment for Play-On-Phone form	The TNEF attachment to play voice messages through the **Play-On-Phone** form.
Multitenant Enabled	This field is disabled.
Use Modular Messaging Style Welcome Menu	The option to provide legacy Modular Messaging TUI welcome menu. When you enable **Use Modular Messaging Style Welcome Menu**, Messaging displays the options to customize prompts. By default, this feature is disabled.

Table continues…

Name	Description
Calling Party Audio Heard During Reach-Me Calls	The audio files that are played to the calling party during Reach-Me calls. The administrator selects the option that plays to the calling party during the Reach-Me process. The options are: • **Silence**: No audio file is played. This is the default option. • **Music**: One or more music files played from a list of Avaya approved music. • **North American Ring Tone**: The audio file that is played for North American customers. • **Custom .wav File**: The audio file that the administrator uploads. When you select the **Music** option, Messaging displays two options: • **Music**: Selects the `.wav` file from the list. • **Play**: Provides an interface to download the `.wav` file from the server to the personal computer of the user. When you select the **Custom .wav File** option, Messaging displays three options: • **Browse**: Launches a file selector window. • **Upload file**: Uploads the selected `.wav` file. • **Play**: Provides an interface to download the `.wav` file from the server to the personal computer of the user. When you try to upload the **Custom .wav File** to the server, Messaging displays a warning. **Warning:** Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to data privacy, intellectual property, including music performance rights, in the country or territory where the Avaya product is used.

Table continues…

Name	Description
Block Message Delivery to Mailboxes when	The option to block Messaging from delivering new messages to locked and uninitialized mailboxes. **Important:** TUI does not inform users that Messaging is blocked from delivering new messages to their mailboxes. If you activate this option, inform users to ensure that message delivery to their mailboxes is not blocked. The options are: • **Not Applicable (Always deliver messages)** • **Mailbox is Locked** • **Mailbox is Locked or Mailbox is Uninitialized (PIN is Unchanged)** • **Mailbox is Locked or Mailbox is Uninitialized (PIN is Unchanged or Greeting not Recorded)** • **Mailbox is Locked or Mailbox is Uninitialized (PIN is Unchanged or Greeting or Name not Recorded)** • **Mailbox is Locked or Mailbox is Uninitialized (PIN is Unchanged or Name not Recorded)** • **Mailbox is Locked or Mailbox is Uninitialized (Greeting not Recorded)** • **Mailbox is Locked or Mailbox is Uninitialized (Greeting or Name not Recorded)** • **Mailbox is Locked or Mailbox is Uninitialized (Name not Recorded)** • **Mailbox is Uninitialized (PIN is Unchanged)** • **Mailbox is Uninitialized (PIN is Unchanged or Greeting not Recorded)** • **Mailbox is Uninitialized (PIN is Unchanged or Greeting or Name not Recorded)** • **Mailbox is Uninitialized (PIN is Unchanged or Name not Recorded)** • **Mailbox is Uninitialized (Greeting not Recorded)** • **Mailbox is Uninitialized (Greeting or Name not Recorded)** • **Mailbox is Uninitialized (Name not Recorded)**

Customized Prompts

Name	Description
Language	The language list for customizing prompts.
Customized prompt	The option to select a type for customizing prompts. Customized prompt list values are: • **MM Style Greeting**: “Hello and Welcome”. • **MM Style Menu**: “Mailbox number, please. For other options, press star (*).” This field also displays the following options: • **Browse**: Launches a file selector window. • **Upload file**: Uploads the selected `.wav` file. • **Play**: Provides an interface to download the `.wav` file from the server to the personal computer of the user. • **Delete**: Deletes the `.wav` file. Prompts are customized at the system-wide level separately for each language and stored in LDAP as `.wav` files in G711 mu-law format.

Minimum TLS versions

Name	Description
LDAP Minimum TLS Version	The minimum TLS version that the LDAP server must use for LDAP TLS communication with remote clients. The default minimum TLS version is TLS 1.0.
IMAP4 Minimum TLS Version	The minimum TLS version that the IMAP server must use for IMAP4 TLS communication with remote clients. The default minimum TLS version is TLS 1.0.
SMTP Minimum TLS Version	The minimum TLS version that the SMTP server must use for SMTP TLS communication with remote clients. The default minimum TLS version is TLS 1.0
POP3 Minimum TLS Version	The minimum TLS version that the POP3 server must use for POP3 TLS communication with remote clients. The default minimum TLS version is TLS 1.0.
User Preferences Minimum TLS Version	The minimum TLS version that the User Preferences web application must use for HTTPS communication with remote clients. The default minimum TLS version is TLS 1.0.

SYSTEM TCP/IP PORTS

Name	Description
LDAP Port	The primary LDAP port. The port number is 389 and cannot be changed. The options are: • **Disable**: Disables access on the corporate LAN. • **Enable**: Enables 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 of the LDAP SSL port. The default is 636. If you change the port number, you must restart the system.
LDAP Front End Alternate Port	The secondary port for LDAP. This port is optional. 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 for directory updates from other Messaging servers in the network. The default port is 56389.
Internal System IMAP4 Port	The internal System IMAP4 port. The port number is 55143. You cannot disable port or change the port number.
IMAP4 Port	The port that the IMAP4 server uses for IMAP4 communication with remote clients. If you click **Enabled**, type the port number that the IMAP4 server uses.
IMAP4 SSL Port	The port that the IMAP4 server uses for IMAP4 SSL communication with remote clients. If you click **Enabled**, type 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**: POP3 clients can access email messaging. • **Disabled**: POP3 email clients cannot access the messaging server. If you click **Enabled**, type the port number that the POP3 server uses for POP3 communication with remote clients. The default is 110.

Table continues…

Name	Description
POP3 SSL Port	The port that the POP3 server uses for POP3 SSL communication with remote clients. The options are: • **Enabled**: POP3 clients can use the POP3 SSL port for more secure access. • **Disabled**: POP3 SSL client access is blocked. If you click **Enabled**, type 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 uses for communication with remote clients. If you click **Enabled**, type 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 communication with remote clients. Use this additional port on the public network instead of, or in addition to, the traditional SMTP port. The system automatically enables this port when you enter a port number. The default status of this port is blank.
SMTP SSL Port	The port that the SMTP server uses for SSL communication with remote clients. If you click **Enabled**, type 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	The option to enable TLS on the outgoing SMTP port that encrypts 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.
Web Client Statistics Port	The port that the System Management Interface uses for collecting Messaging Web Access statistics from the application servers. You cannot change the port number.

RESCHEDULING INCREMENTS FOR FULL MAILBOX DELIVERY

Name	Description
Increment fields	The incremental interval in days, hours, and minutes during which the system waits to resend messages. When the mailbox is full, the system waits and resends the messages according to the incremental interval. When the system reaches a zero increment, the system does not deliver messages. You can specify maximum 10 rescheduling increments to reattempt delivery of a message to a full mailbox. If you set any increment value to 0, then the system turns off the rescheduling of the message deliverables.

Related links

Changing user properties on page 191
Adding a trusted server on page 155

Setting up community sending restrictions

About this task

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

Sending Restrictions applies to only Voice Mail messages. You create a community to prevent members from:

- Sending mail to other groups

Procedure

1. Open a web browser and in the **Address** field, type the IP address or FQDN of the Messaging System Management Interface.
2. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Sending Restrictions**.
3. On the Edit Sending Restrictions page, select the checkboxes to establish sending restrictions between communities of users. If a checkbox is selected, the corresponding sender community (row) cannot send voice mail to members of the corresponding recipient community (column).
4. Click **Save**.

Adding a network server

About this task

Use the Networked Servers webpage to connect Messaging to a different network environment. For example, a Message Networking environment. 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 webpage, select an LDAP server.
3. Click **Add a New Networked Server**.
4. On the Add Networked Server webpage, enter the appropriate information in the fields.
5. Click **Save**.

Next steps

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

Related links

Add Networked Server field descriptions on page 171

Add Networked Server field descriptions

Name	Description
Server Name	The name of the server that you want to add.
Password	The password for directory updates.
Confirm Password	The field to confirm the password that you entered in the **Password** field.
IP Address	The IP address of the server that you want to add.
Server Type	The type of server that you want to add. Except for the local server, the server type for all servers is LDAP.

Table continues…

Name	Description
Mailbox Number Length	The length of the long mailbox number that you can select from the drop-down list. The options are: • **Variable**: For different lengths. • Any number from 3 to 50: For fixed lengths.
Default Community	This field is unused.
Updates In	Specify whether the local server accepts directory updates from the remote networked server. The options are: • **yes**: Accepts directory updates from the networked server. **no**: Blocks directory updates from the network sever, regardless of the setting of this option on the networked server that sends updates. **Note:** If you are administering the local server, this field controls updates on a systemwide basis.
Updates Out	Specify whether the local server can send updates about users to the specified networked server. **Note:** If you are administering the local server, this field controls updates on a systemwide basis.
Remote LDAP Port	The port that Messaging uses to connect to the networked server and send directory updates. The default port is the port that you specify in **LDAP Directory Update Port** on the System Administration webpage.
Inbound LDAP Security	The type of encryption required for the connection between the storage server and the networked server for inbound LDAP directory updates. When you set the **Updates In** field to *no*, Messaging prevents the networked server from updating the LDAP directory without using the specified level of security. The options are: • **Must use SSL**: Requires SSL encryption for updates. • **Must use SSL or encrypted SASL**: Requires either SSL or SASL encryption for updates. The default value is **Must use SSL or encrypted SASL**.

Table continues…

Name	Description
Outbound SMTP Port	The port that Messaging uses to connect to the networked server. The default port is 25. Messaging supports secure SMTP by using TLS on the outbound SMTP port.
Outbound SMTP Service	The type of SMTP service required for the connection between the storage server and the networked server. The options are: • **SMTP (Use TLS if available)** **Secure SMTP (Using TLS)** Messaging supports only **SMTP (Use TLS if available)** for incoming connections from Modular Messaging and Message Networking.

Telephone Number Mapping

When a local user receives a call-answer message, the system attempts to match the calling party number or CPN of the sender to a user number in the database.

Name	Description
Enable Telephone Number Mapping	Map the CPN of a sender to the number of a recipient. • **yes**: Messaging maps the CPN of the sender to the number of the recipient through a lookup table. • **no**: Messaging does not identify recipients as users in the Messaging network. If you change this option from **yes** to **no**, Messaging deletes all mappings from the local database and sets the telephone numbers for all users associated with the network server to **null**.

Table continues…

Name	Description
Map From	Administer Messaging to compare the digit string that you enter in this field with the base numbers of a user. When the value in the **Map From** field matches the initial digits of the base number, Messaging creates a mapped telephone number by: • Stripping the matching digits from the base number. • Prefixing the number in the **Map To** field to the base number. If the **Map From** field is empty, Messaging compares incoming CPNs to all base numbers. Messaging supports more than one set of **Map From** and **Map To** numbers with different lengths. The valid values are from 0 to 50.
Map To	The digit string that Messaging prefixes to the base number after Messaging strips the digits that match the digits in **Map From**. When **Map To** is: • **Empty**: Messaging does not prefix digits to the base number after the digit stripping. • **none**: Messaging sets the matching telephone number to **null**. The **Map To** values can be of different lengths up to a maximum of 50 digits.
Add Mapping	The mapping to add to the mapping table.
Delete Mapping	The mapping to delete from the mapping table. Mappings cannot be modified. Messaging supports only deleting a mapping and creating a new mapping.

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.

Table continues…

Name	Description
Total Subs	The number of users associated with the network server.

Report of Network Servers field descriptions

Name	Description
Server Name	The name of each network server.
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.

Table continues…

Name	Description
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 webpages from the navigation pane of a dedicated application server.

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

Fax overview

Messaging supports sending and receiving faxes. You can send faxes from Windows applications to individual fax numbers.

You can:

- Enable or disable the fax feature.
- Enable or disable the email notification for the outbound fax.
- Enable or disable encryption of the fax transmission between application servers.
- Change the number of SIP sessions that Messaging supports for the outbound fax.
- View the status of the outbound fax in the queue.
- Run a diagnostic test to verify the administration of the fax feature.
- Receive faxes using:
  - **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.

Note:

To send faxes, the Internet printing feature must be enabled on the computers of users. If this feature is not enabled, Windows displays an error message to users who try to send faxes through Messaging.

Messaging supports a maximum of 20 simultaneous ports for incoming and outbound fax transmissions. For example, if Messaging is receiving faxes through all the 20 ports, Messaging can send faxes only after a port is available.

Outbound fax limitations

Messaging supports a maximum of 500 outbound fax transmissions in the fax printer queue and a maximum size of 150 MB for each fax transmission. If users try to send more faxes and the fax printer queue exceeds 500 fax transmissions or if the users try to send a fax transmission that exceeds 150 MB, Messaging denies the request, and the Windows printer application displays an error message to the users.

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 User List and Global Address List 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.

Configuring system parameters

About this task

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 requiring further modification. You can also 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.
3. Click **Apply**.
4. In the confirmation dialog box, click **OK**.

   Repeat this procedure on each application role in the cluster.

System Parameters field descriptions

Name	Description
Avaya Branding Tone	The Avaya branding tone that Messaging plays 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:

Name	Description
Include caller ID in subject line	The option to include the caller ID in the subject line. The options are: • **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	The prefix that the system adds to the subject line of an original message. For example, `Original messages`. The text content is the caller ID and contact name.
Intro text in subject line of message replies	The prefix that the system adds to the subject line of replies. • For example, `RE [Subject line]` Users can customize the subject line for replies.

Table continues…

Name	Description
Intro text in subject line of forwarded messages	The prefix that the system adds to the subject line of forwarded messages. • For example, `FW [Subject line].` Users can customize the subject line for forwarded messages.

Login Announcements:

Name	Description
Maximum length of login announcement	The maximum length of the login announcement that users can record. The maximum length of the login announcement can be 4,500 seconds, and the default value is 120 seconds.

Recording Times:

Name	Description
End-of-recording silence	The duration of silence that indicates the end of the recording. The default duration is 4 seconds. The maximum duration is 30 seconds. **Note:** When you set **End-of-recording silence** to 0 seconds, the system stays in the recording state infinitely until the caller ends the recording.
End-of-recording silence for TTY input	The duration of silence that indicates the end of the recording in the TTY mode. The default duration is 10 seconds. The maximum duration is 30 seconds. **Note:** When you set **End-of-recording silence for TTY input** to 0 seconds, the system stays in the recording state infinitely until the caller ends the recording.
VoIP DTMF cut-off time	For VoIP integrations only. The cut-off time, in milliseconds, at the end of a recording that DTMF ends. The default is 150 milliseconds.

Call Sender and Transfer:

Call transfer operations such as Call Sender, Auto Attendant, and Transfer to Extension use the call attempt time-out parameter for both internal calls and external calls.

Name	Description
For internal calls, a call attempt times out after	The number of seconds that elapse before the telephony server sends an internal call 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 Ring No Answer (RNA). If you configure the time out value at the system level on the telephony server, you can check your telephony server for a typical setting. The maximum value is 60 seconds.
For external calls, a call attempt times out after	The number of seconds that elapse before the telephony server sends an external call to voice mail. The default is 45 seconds. During call transfer-initiated calls, prevent a call going to voice mail by lowering the time out value. This value must be lower than the time taken by a call to an external telephone number to roll over to voice mail in RNA cases. The maximum value is 60 seconds.

Play on Phone:

Name	Description
Time out (on no answer) after	Period of time, in milliseconds or number of rings, after which the system ends the call if you do not answer a Play on Phone 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 16,000 milliseconds and the maximum is 999,999,999 milliseconds. The two units are : • Milliseconds • rings

Ringback:

Name	Description
Number of seconds between outgoing ringback tones	The number of seconds that an outgoing ringback tone takes. The default is 5 seconds.
First ringback timeout	The time to wait, in milliseconds, for the first ringback. The default is 15,000 milliseconds.

Table continues…

Name	Description
Ringback timeout	The time to wait, in milliseconds, for the ringback to end. The default is 7,000 milliseconds.

Nightly Maintenance:

Name	Description
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. You must stagger the nightly maintenance among the application servers. The default time is 03:37 a.m.

Restrictions for Callers:

Name	Description
Allow callers to reach the system main menu	The option that a caller uses 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. When the extension number 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. When the extension number does not have an associated mailbox or a caller application, Messaging disconnects the call. The default is **yes**.
Allow callers to skip greeting by pressing #	The option for a caller to skip the call answering greeting by pressing the hash (#) button. The default is **yes**.

Table continues…

Name	Description
Play record instructions to callers after a greeting	The option determines whether Messaging plays recording instructions after a call answering greeting. The options are: • **yes**: After a call answering greeting, Messaging plays the prompt “Record your message after the tone. When you have finished, you can hang up or press 1 for more options.”. • **no**: Messaging skips this prompt. The default is **yes**.

Storage Synchronizer:

Name	Description
Maximum length of the storage synchronizer queue	The maximum number of messages in the storage synchronizer queue. When the maximum size is reached, users cannot leave call answer messages. The default value is 200 messages. **Note:** This is an advanced setting. Consult your account representative before editing this setting.

Messaging Web Access:

Name	Description
Subscriber Access Port	The port for subscriber access. The default port is 10100.
Subscriber Access Protocol	The protocol for subscriber access. The options are https: and http:. The default protocol is https:. Messaging supports http: only if a customer-provided load balancer is used for Messaging Web Access.
Web Notification Service Port	The service port for web notifications. The default port is 8443.
Minimum TLS Version	The minimum TLS version that is required to access Messaging Web Access. If your browser does not support the selected TLS version, you cannot use Messaging Web Access. The default TLS version is 1.0.
Instant Notification	Instant notifications of new messages.
Remember Me	The option to remember the credentials of users.

Table continues…

Name	Description
Remember Me Expiration	The number of days that Messaging Web Access remembers the credentials of users. The default number of days is 30 days.
Session Expiration	The number of hours after which the Messaging Web Access session expires. The default number of hours is 8 hours.
Control disable time during phone operations	The number of seconds after which Messaging Web Access disables web access controls during phone operations. The default is 15 seconds.

Fax:

Name	Description
Fax detection time-out	The duration, in milliseconds, that the application server detects fax tones after accepting a call. The default duration is 20,000 milliseconds. If a site has multiple languages and a user records a long greeting, the greeting might cause the fax detection time-out to expire. For example, if User A, wants to send a fax to User B, then User A waits for the prompts to play, and then sends the fax. The fax detection time-out might expire and the application server might not detect the fax. Consider the impact of a long greeting, and set a time-out value that is longer than the duration between the first prompt and the beep tone.

Detect and transfer to fax server settings:

Name	Description
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 applicable only if you set the **Fax receiving** option as **Detect and transfer to fax server**.
Destination identification during transfer	The fax destination, which is a mailbox or a primary extension. The default is Mailbox. This field is applicable only if you set the **Fax receiving** option as **Detect and transfer to fax server**.

Table continues…

Name	Description
DTMF following destination identification	The method to prefix a DTMF qualifier to a fax destination number, so that the fax server receives complete fax destination identification number. The options are: • **Asterisk (*)** • **Hash (#)** • **None ()** The default is **None**. This field is applicable only if you set the **Fax receiving** option as **Detect and transfer to fax server**.

Receive and forward to email settings:

Name	Description
Intro text in subject line of Fax messages	The text that is present in the subject line of fax messages. This field is applicable only if you set the **Fax receiving** option as **Receive and forward to email**.
Fax recording format	The options are: • **PDF (Portable Document Format)**: When the system receives 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. • **TIFF (Tagged Image File Format)**: When the system receives 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. The default format is TIFF. This field is applicable only if you set the **Fax receiving** option as **Receive and forward to email**.

Related links

Load balancing Messaging Web Access on page 458

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.

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings (Application)** > **Cluster**.
2. Enter the appropriate information in the fields.
3. Click **Apply**.
4. In the confirmation dialog box, click **OK**.

Related links

Configuring a cluster on page 110
Cluster field descriptions on page 111

Configuring storage capacity for offline call answering

Procedure

1. On the **Administration** menu, click **Messaging** > **Server Settings** > **Server Role / AxC Address**.
2. In the **Disk usage quota** field, enter the information in bytes.

   The default is 25 GB.

   Note:

   This is an advanced setting. Consult your account representative before you enter information in **Disk usage quota**.
3. In the **Delete cached voice messages from the cache after** field, enter the time in hours.

   The default is 72 hours.

   Do not increase the default time in **Delete cached voice messages from the cache after** without increasing the value in **Disk usage quota**. The increase in the time increases the number of voice messages stored in the cache, which might consume the default disk storage quota of 25 GB.

   To prevent this, you must check your current usage in the **Cache Storage Usage** field.
4. Click **Apply**.

   The system displays a confirmation message.
5. Click **OK**.

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. Change the external SMTP host server.
2. Change the mail gateway.

Related links

Administering the external SMTP host on page 76
Adding a mail gateway on page 77

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 webpages from the navigation pane of the dedicated application server.

To open storage-role webpages, 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 webpage 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 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.

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 with 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 about the caller.

You can create mapping tables when you add a network server to your system.

Remote updates

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

Ensure that the administrator for each remote system in your voice mail network agrees to take remote updates from your local system. You must then update the list of remote users on your local system regularly.

Related links

Defining dial rules on page 125
Adding a network server on page 171
User Management field descriptions on page 193
Defining dial rules on page 125
Adding a network server on page 171
User Management field descriptions on page 193

Password complexity enhancement for Subscriber Mailbox

The following are the rules for creating a password for Subscriber Mailbox:

- The password must not match the mailbox number.
- The password length must be greater than or equal to the minimum administered length on the System Administration SMI screen.
- If the number of digits in the password is greater than one:
  - All the digits of the password must not be the same.
  - All the digits of the password must not be consecutive. For example, you cannot use 3456. However, you can use 34568.

- All the digits of the password must not be in the descending order. For example, you cannot use 5432. However, you can use 5431.

- If the number of digits in the password is greater than three:
  - The password must not be a subset of the mailbox number. For example, if the mailbox number is 53010, the password cannot be 3010.
  - The password must not be a subset of the reverse of the mailbox number. For example, if the mailbox number is 53010, the password cannot be 0103.
  - The mailbox number must not be a subset of the password. For example, if the mailbox number is 3010, the password cannot be 53010.
  - The mailbox number must not be a subset of the reverse of the password. For example, if the mailbox number is 3010, the password cannot be 50103.

Manage local users

Adding users

About this task

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

If you use Exchange Server as a storage server, you can add the existing users in Active Directory directly to Messaging without manually configuring the user values.

You cannot add users if the storage destination is Exchange and any of the following conditions are true on the System Administration webpage:

- 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 webpage, click **Add**.
3. Enter the appropriate information in the fields.
4. Click **Save**.

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

Related links

Adding users from Active Directory to Exchange Server on page 190

Assigning an attendant number on page 128
User Management > Properties field descriptions on page 194

Adding users from Active Directory to Exchange Server

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 Server and any of the following conditions are true on the System Administration Web page:

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

You also cannot add users whose user names contain more than 27 characters. You must manually add these users.

Before you begin

- You have configured the Exchange Server storage destination.
- 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.
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 1235.

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 Administration webpage:

- 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 webpage. However, this page does not have filters that assist you in locating a specific user.
3. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
4. In the **Edit User/Info Mailbox** section, in the **Identifier** field, type the user identifier and click **Edit**.

   The system displays **User Management** > **Properties** webpage.
5. Change the user information as appropriate.
6. Click **Save**.

   The system saves the user properties.

Related links

System Administration field descriptions on page 159
User Management > Properties field descriptions on page 194

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 webpage. However, the User Management webpage does not have filters that assist you in locating a specific user.
3. Log in to the Messaging SMI, and click **User Management**.
4. On the User Management webpage, in the **Identifier** field, type the identifier, and then click **Edit**.
5. On the User Management > Properties webpage, click **Delete**.
6. In the confirmation screen, click **OK** to continue.

   The system deletes the user.

Related links

User Management > Properties field descriptions on page 194

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 that you pronounce the name.

For increased speech recognition accuracy, Messaging supports Nuance Recognizer 10 and Vocalizer 6 for Text-To-Speech.

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

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

You will not find a search order between these fields. A match is a match. You must use the **Pronounceable name** field to increase speech recognition. For example, if the primary language of your system is English, spell Dan DuBois as `Dan Doobwah`. You can use the other fields to increase the recognition rate.

You can also enter an alternate name for the user. For example, William Bell might also be known as Bill Bell. In the User Properties webpage, 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. For the speech recognition feature, you must administer the same default language for all the sites. These sites must be on the selected list of Additional sites included in the directory in Auto Attendant.

For Speech Auto Attendant, ensure that you specify the names of the users in a language that matches the default language setting of the site to which the user belongs.

For example, if the default language for a site is U.S. English, then specify the name of the user belonging to the site in U.S. English only.

User Management field descriptions

License Status

Name	Description
License mode	The license modes include: • Normal • Restricted • Error

Edit User / Info Mailbox

Name	Description
Identifier	The mailbox number or the email address of the user whose properties you want to edit.

Add User/Info Mailbox

Name	Description
Add a new user	The option to add a new user.
Add a new Info Mailbox	The option to add a new info mailbox.

Add User by AD lookup

This section is available if you configure the Exchange storage destination.

Name	Description
AD search	To do an Active Directory search, the Messaging system provides the following options: • Active Directory field name • Comparator • Text field You can do an Active Directory search using any of the following: • mail • telephone number • name **Note:** When you set the password, and the password does not meet the configured PIN policy, the system displays a validation error message. For example, `Cannot create subscriber. The Default Exchange and CallPilot User Password is contained within mailbox number.`

User Management > Properties field descriptions

User Properties

The following table contains information about the settings you can configure when you are creating a new user or modifying an existing user. When you are modifying an existing user, Messaging also displays the Advanced Tasks and User Preferences sections.

Name	Description
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. The Speech Recognition and Text-To-Speech features also use **Display name** to identify and pronounce the name of the user.
ASCII name	The name that contains only ASCII characters. If **First name** and **Last name** contain: • Only ASCII characters, Messaging automatically populates the ASCII name in the `Last name, First name` format.

Table continues…

Name	Description
	• Both ASCII characters and other characters, you must enter an ASCII name in the `Last name, First name` format. The Spell Name feature requires that the ASCII name starts with the last name. When a caller uses the Spell Name feature to connect to a user, Messaging locates the user by the name that you enter as the ASCII name.
Site	The site to which the user belongs. When you select the site of the user, Messaging automatically displays the site identifier next to the **Mailbox number** field and a static label of the identifier next to the **Extension** field. The list contains all administered sites. The default value is **Default**.
Storage destination	The option to specify the storage server. The options are: • Avaya Message Store • Microsoft Exchange If you select **Microsoft Exchange**, then SMI displays the **Exchange email address** and **Exchange server FQDN** fields.
Mailbox number	The mailbox number of the user. All mailbox numbers must be unique. When you select the user site in the **Site** field, Messaging automatically populates the corresponding preceding digits of the mailbox number. You can overwrite these digits.
Email address	The email address of the mailbox of the user.
Numeric Address	The unique identifier that users provide to address messages within the voice mail network. The numeric address can contain the mailbox number. 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.
Extension	The telephone extension of the user. The extension length must match the telephony style and the short extension length of the site. Usually, the extension is unique. If you share the extension with another user, Messaging displays the name of both users and prompts callers to select the required mailbox.
Include in Auto Attendant directory	The option using which the Messaging system adds the user to the Auto Attendant directory.

Table continues…

Name	Description
Additional extension	The additional extensions that 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 maintain both the old and the new extension in the internal directory. If you select **Auto login** on the User preferences page, the user can choose which additional extensions log in automatically. You can activate **Auto login** only if **Allow auto login** is selected for the class of service of the user.
Class of Service	The CoS of the user. The CoS controls user access to features and provides general settings such as mailbox size.
Community	The option to configure community for users.
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 of your system. To increase the likelihood of the Speech Recognition feature recognizing the name, spell the name as you 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 can also be pronounced 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: • **No**: When the user has a voice mailbox only. • **ByCOS**: When the CoS controls how the system enables MWI. The **MWI enabled** field overrides the MWI setting defined by the CoS to which the user is associated.
Miscellaneous	Additional information about the user. In the Messaging system, you can find a value in the **Miscellaneous** field on the SMI page.
New password	The password that the user must use to log in to the Messaging mailbox.

Table continues…

Name	Description
	Passwords must follow the complexity rules for subscriber mailbox. For more information, see *Password complexity enhancement for Subscriber mailbox*. If you do not enter a value for an existing user, the system does not change the existing password. **Note:** When you set the password, and the password does not meet the configured PIN policy, the system displays a validation error message. For example, `Password consists solely of consecutively increasing digits. LDAP Error 1501.`
Confirm password	The password that the user must enter to confirm 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 login	The option to enable the user to change the password when users call the voice mailboxes the next time. Messaging requires that new users change the temporary passwords when users log in to the mailbox for the first time.
Voice messaging password expired	The option to enable the user to continue using the password even after the password expires. If a user password expires, Messaging enables the option.
Locked out from the Messaging system	The option to prevent the user from accessing the Messaging system. The options are: • **Unlocked**: The administrator can unlock the mailbox by selecting the **Unlocked** option. When the mailbox is unlocked by the administrator, the **Locked Out due to excessive Invalid Login Attempts** option is disabled in the system. • **Locked Out by Administrator**: The administrator locks the mailbox by selecting the **Locked Out by Administrator** option. In this case, the auto-unlock feature is not enabled in the system. • **Locked Out due to excessive Invalid Login Attempts**: Messaging automatically locks the system when a user fails to enter proper login credentials after a certain number of consecutive failed attempts. In this case, the **Locked Out due to excessive Invalid Login Attempts** option is enabled in the system. The number of consecutive failed attempts are specified on the **Consecutive Invalid Attempts** field on the System Administration webpage. If the auto-unlock feature is enabled in the system, the

Table continues…

Name	Description
	Unlocked option is selected after the **Lock Duration time** elapses.
Advanced Tasks	
Reset the message waiting indicator for extension	The button to reset the MWI on your desk phone. When you receive a voice message, the MWI light turns on. The MWI light turns off when the user either listens to the message using the phone or marks the message as read in Outlook. In some cases, the MWI light might not indicate a correct status of user's voice messages. The **Reset** option enables the administrator to fix this issue. This option is only available when you are editing an existing user. If the MWI light cannot be reset, Messaging displays the `Message waiting light cannot be reset` error.
User Preferences	
Open User preferences	The option to configure additional user settings, such as user language or call notification options. This option is only available when you are editing an existing user.

Exchange Properties

SMI displays the fields **Exchange email address** and **Exchange server FQDN** only if you select **Microsoft Exchange** in Storage Destination.

Name	Description
Exchange email address	The email address of Exchange Server.
Exchange server FQDN	The FQDN of Exchange Server.

Related links

Setting the length of the mailbox number on page 69
Configuring the postmaster mailbox number on page 71
Sites field descriptions on page 53
Setting the site properties for the first time on page 50
Class of Service overview on page 213

Assigning Messaging Web Access to users

About this task

As an administrator you must assign the Messaging Web Access feature to a particular CoS. So that, all users of that particular CoS gains access to Messaging Web Access. By default, the Messaging Web Access feature is inactive.

Use this procedure to assign the Messaging Web Access feature to a CoS in SMI.

Important:

If DNS does not contain a record of the IP address of Messaging Web Access in the FQDN format, users cannot gain access to Messaging Web Access.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. In **Class of Service**, select the appropriate CoS.
3. In the **General** section, select **Allow Messaging Web Access**.
4. Click **Save**.
5. Repeat steps 3 to 5 for each CoS to which you want to assign the Messaging Web Access feature.

Configuring system policies

Procedure

1. Log in to the server that is running the storage role by using privileged user account and password.
2. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Policies**.
3. Enter the appropriate information in the fields.
4. Click **Save**.

   The system saves the details.

Related links

System Policies field descriptions on page 199

System Policies field descriptions

Name	Description
Default Exchange and CallPilot User Password	

Table continues…

Name	Description
Password	The default Exchange user password. **Note:** When the user sets the password, and the password does not meet the configured PIN policy, the system displays a validation error message. For example, `Default Exchange user password cant be same digit repeated.`
Hide default password	The option to hide the default password.
Caller Applications Administrator	
Password	The password for accessing Caller Applications Editor.
Confirm password	The option to confirm the password for accessing Caller Applications Editor.
Notify Me E-Mail Customization	
Language	The option to customize the body of the Notify Me email notifications for each language installed on the system.
Custom Text	Localized text that replaces the home site external messaging access number of the user in Notify Me email notifications for the selected language. For example, an administrator can add an access number for each site that a multisite system supports. When you make changes to the text, you must restart Messaging for the changes to take effect.

Notify Me email customization

You can customize the content of Notify Me email notifications to meet the needs of the organization.

The default content of these notifications include the external Messaging access number for the site to which the user belongs. Administrators can, for example, add an access number for each site that a multisite system supports. Administrators can also localize the content.

Configuring email customization of Notify Me

About this task

Use this procedure to customize the notify me email body.

Before you begin

Ensure that you have the notifymeCallbackNumberOverrideText entry in the `aic-settings.properties` file enabled.

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **System Policies**.
2. On the System Policies page, in the **Custom Text** field, enter the custom Messaging access number.

   For multi-line notify me, you must enter the line feed characters. Only users having english language configured will receive notify me messages with the custom text.
3. Click **Save**.

   The system displays a message `You need to restart Messaging for some of these changes to take effect`.

Manage info mailboxes

Info mailbox overview

Info Mailbox is the default name of the CoS that controls the maximum length of a recorded message in an info mailbox. An info mailbox plays greetings and provides information to a caller. However, a caller cannot leave a message in the 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 webpage.

An info mailbox includes:

- 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.

Related links

Changing a Class of Service on page 214

Adding an info mailbox

About this task

Use this procedure to add the Info Mailbox CoS to each user so that each user can create a message for an information mailbox.

A typical informational message includes details about directions, business hours, weather, or human resources information. You can record messages for up to five minutes.

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.
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.

Related links

Properties for New Info Mailbox field descriptions on page 202

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 name of the info mailbox in the Auto Attendant directory that is a Text-to-Speech playback of the display name.
ASCII name	The ASCII name that contains only ASCII characters. If **First name** and **Last name** contain: • Only ASCII characters, Messaging automatically populates the ASCII name in the `Last name, First name` format. • ASCII characters and other characters, you must enter an ASCII name in the `Last name, First name` format.
Site	The name of the site of which the info mailbox is a member.

Table continues…

Name	Description
Mailbox number	The mailbox number of the info mailbox. All mailbox numbers must be unique. Avaya recommends the E.164 international numbering plan because E.164 ensures that each telephone extension and voice mailbox combination is unique across all sites in your enterprise. Messaging also supports non-E.164 numbering plans. So if each mailbox number is unique, you can continue to use your existing numbering plan. For easy mailbox administration, assign each user a mailbox number that matches their telephone extension.
Email address	The email address of the info mailbox.
Numeric Address	The unique identifier that users provide to address messages within the voice mail network. 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.
Extension	The telephone extension of the info mailbox. The extension length must match the site length.
Include in Auto Attendant directory	The option to add the mailbox to the Auto Attendant directory.
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 must be maintained in the internal directory.
Class of Service	The CoS of the info mailbox, usually *Info Mailbox*. CoS controls user access to features and provides general settings such as mailbox size.

Table continues…

Name	Description
Pronounceable name	The name of an info mailbox that the Speech Recognition feature pronounces. The spelling might differ from the pronunciation. To increase the likelihood of the Speech Recognition feature recognizing the name, spell the name as you 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 extension number that you enter.
New password	The password to log in to the Messaging mailbox. Passwords must follow the complexity rules for subscriber mailbox. For more information, see *Password complexity enhancement for Subscriber mailbox*. If you do not enter a value for an existing info mailbox, the system does not change the existing password. **Note:** When you set the password, and the password does not meet the configured PIN policy, the system displays a validation error message. For example, `Password involves consecutively decreasing digits. LDAP Error 1491.`
Confirm password	The option to confirmation the value in the **New Password** field. Enter a password only if you are adding a new password or changing an existing password.

Table continues…

Name	Description
User must change voice messaging password at next login	The option to force users to change passwords the next time that the users call in to their info mailboxes. By default, Messaging requires that new users change the temporary passwords at first login.
Voice messaging password expired	The option for the user to continue using an expired password. If a user password expires, Messaging enables the check box. Clear the check box to continue using the expired password.
Locked out from the Messaging system	The option to prevent user access to the Messaging system. The options are: • **Unlocked**: The administrator can unlock the mailbox by selecting the **Unlocked** option. When the mailbox is unlocked by the administrator, the **Locked Out due to excessive Invalid Login Attempts** option is disabled in the system. • **Locked Out by Administrator**: The administrator locks the mailbox by selecting the **Locked Out by Administrator** option. In this case, the auto-unlock feature is not enabled in the system. • **Locked Out due to excessive Invalid Login Attempts**: Messaging automatically locks the system when a user fails to enter proper login credentials after a certain number of consecutive failed attempts. In this case, the **Locked Out due to excessive Invalid Login Attempts** option is enabled in the system. The number of consecutive failed attempts are specified on the **Consecutive Invalid Attempts** field on the System Administration webpage. If the auto-unlock feature is enabled in the system, the **Unlocked** option is selected after the **Lock Duration time** elapses.

Related links

Sites field descriptions on page 53
Setting the site properties for the first time on page 50
Class of Service overview on page 213

Manage mailboxes

Adding a mailbox

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.
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.

Resetting the voice mailbox password

Procedure

1. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.
2. Use the built-in filters to find 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 webpage. However, the User Management webpage does not have filters to locate a specific user.

3. On the User Management > Properties webpage, in the **New password** field, type a password that the user must use to log in to the Messaging mailbox.

   Passwords must follow the complexity rules for subscriber mailbox. For more information, see *Password complexity enhancement for Subscriber mailbox*. If you do not enter a value for an existing user, the system does not change the existing password.

   Some browsers automatically populate web-based forms with passwords. If **New password** contains a value, clear the field and enter the password. To prevent Messaging from automatically populating the passwords, turn off the option to remember the password in your browser.

4. In the **Confirm password** field, reenter 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.

   Even if you do not enter a new password in Step 3 and Step 4, you can still save the updated user details without any error. Your browser displays the following message after you click **Save**:

   ```
   You have updated the subscriber details.
   ```

Unlocking the voice mailbox account

Procedure

1. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.
2. Use the built-in filters to find 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 webpage. However, the User Management webpage does not have filters that assist you in locating a specific user.

3. On the User Management > Properties webpage, select the **Unlocked** option.

   When the mailbox is unlocked by the administrator, the **Locked Out due to excessive Invalid Login Attempts** option is disabled in the system.

   By selecting the **Unlocked** option, the user can use the correct login credentials to log in to the voice mailbox at the next logon. Messaging automatically locks the mailbox when the user fails to enter proper login credentials after a certain number of consecutive failed attempts.

   Using the **Consecutive Invalid Attempts** field on the System Administration webpage, you can set the number of consecutive failed attempts for the system.

4. Click **Save**.

   The system saves the settings.

   If a user still receives the following message, the Exchange Server mailbox of the user might be deleted:

   ```
   Too many invalid login attempts
   ```

5. **(Optional)** Check whether the mailbox of the user exists.

Related links

Messaging displays the Too many invalid login attempts message on page 560

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.
  - Manually administer a remote user instead of waiting for a remote update.
- 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.

Related links

Remote updates on page 209
Running a remote update manually on page 211

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 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 cannot manually enter remote user information. Before you administer your user or remotely update information, consult the remote system administrators in your network. Each remote system administrator must determine whether to use remote updates.

Types of remote updates

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 new users to the network. Complete updates might involve thousands of users and require heavy system resources. Therefore, you must perform complete updates during nonprime time to reduce the impact on system users.

Additionally, the local Messaging system can automatically schedule a complete update during nonprime time from a remote system if the local system detects discrepancies among databases.

Partial updates

Partial updates occur regularly to add or change user information. 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 are configured for remote updates, the system with any change in user database notifies the other systems in the network.

Setting up remote updates

About this task

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

Before you begin

Ensure that:

- The administrator for each remote system agrees to take remote updates from your local system.
- Your local server connects to at least one remote server.

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 webpage 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. In the **Updates In** field, click **yes**.
5. In the **Updates Out** field, click **no**.
6. Click **Save**.

The system modifies the server information successfully.

7. To receive remote updates, repeat the procedure on each networked server.

Related links

Adding a network server on page 171

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 webpage, click *Feature* from the **Type** 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 webpage, click a server from the list.
8. Click **Request Update**.

   Tip:

   Click **Refresh Update Status** to verify the status of the update.
9. Return to the Messaging Measurements webpage 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 webpage, 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.

Chapter 9: Class of Service

Class of Service overview

Using CoS, you can define the privileges and features assigned to a group of users.

- Use the Class of Service webpage to define each CoS, create a new CoS, and change an existing CoS. You can create maximum 512 CoS. The maximum storage size for CoS is 262,136 KB.
- Use the User Management webpage to assign a previously defined CoS to a user.

Default CoS:

Messaging has the following default CoS that you can assign to each user:

- **Standard** or **Enhanced**: For local and domestic long distance calls.
- **Executive**: For local, domestic long-distance, and international calls.
- **Info Mailbox**: To create a message for an information mailbox. A typical information message includes details about directions, business hours, the weather, or human resources. You can record messages of maximum 5 minutes for an information mailbox. You cannot create an information mailbox by assigning the Info Mailbox CoS to the user. An information mailbox does not require a seat license.
- **Administrator**: For users to send. A login announcement includes announcements or instructions from the system administrator about the voice mail system. This CoS is unrelated to the administrative privileges managed through the Server (Maintenance) RBAC administration. Messaging supports two levels of login announcements:
  - Cluster level: To record login announcement that Messaging sends to users in all sites administered in an application server cluster. In a multisite deployment where the application servers are not added to a cluster, Messaging sends the login announcement only to the sites administered on the same application server.
  - Site level: To record login announcement that Messaging sends to users administered on the same site of an application server.
- **Postmaster**: To create a postmaster mailbox. The postmaster mailbox is a systemwide mailbox dedicated for the postmaster, which manages the emails for a site.
- **ELA**: For the Enhanced-List Application.

Related links

Adding an info mailbox on page 201
Class of Service field descriptions on page 216

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 webpage, click **Add New**.
3. Enter the appropriate information in the fields.
4. Click **Save**.

   The system saves the details.

Related links

Class of Service field descriptions on page 216

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. In the **Class of Service** field, click the CoS that you want to change.
3. Make your changes.
4. Click **Save**.

The system saves the changes.

Related links

Class of Service field descriptions on page 216

Deleting a Class of Service

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. In the **Class of Service** field, click the CoS.
3. Click **Delete**.

   The system displays a confirmation dialog box.
4. Click **OK**.

   The system deletes the CoS.

Basic and Mainstream mailbox licensing

Messaging offers a cost-effective licensing model for customers who want only the basic messaging features in the form of a lower-cost Basic mailbox license. Customers who want advanced capabilities can buy the Mainstream mailbox licenses.

- Basic: Provides the basic call answering, voice messaging functionality, and IMAP access to the Avaya message store.
- 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 access to Messaging Web Access.

  Note:

  To increase the system capacity to either 30,000 or 40,000 local users, you must restrict access to Messaging Web Access and end-user use of external IMAP4 and POP3 clients. For 40,000 local users, disable the following features:

  - Reach Me
  - Notify me
  - Transfers

Administrators can use a mix of the Basic and Mainstream seat licenses on Messaging.

Note:

You can enable or disable media encryption in Messaging by administering the **FEATURE MEDIA ENCRYPTION FEAT_MSG_ME** option when you generate the PLDS license. If you disable media encryption, you cannot enable the encryption later.

Class of Service field descriptions

Name	Description
Class of Service	The name of the class of service. The standard options are: • Standard • Enhanced • Executive • Info Mailbox • Administrator • Postmaster • ELA This field has the following two buttons: • **Add New**: To select a new class of service. • **Delete**: To delete an existing class of service.

General:

Name	Description
Name	A customized name for the class of service. Enter a descriptive name instead of a number.
ID	The unique identification number of the class of service.

Table continues…

Name	Description
Required seat license	The type of seat license required for users who are members of the class of service. The options are: • Basic (VALUE_MSG_SEAT_BASIC) • Mainstream (VALUE_MSG_SEAT_MAINSTREAM) The Mainstream license is required only for the following Messaging features: • Reach Me • Notify Me - Text message or page notification - Phone call to a telephone or mobile phone - Email • Fax - Detect and transfer to fax server - Receive and forward to email • Access to Messaging Web Access • Speech-based features - Speech recognition for addressing - Basic Speech Auto Attendant - Access to Avaya one-X® Speech Messaging does not display this field for a new class of service.
Telephone User Interface	The TUI options for users assigned to the class of service. The options are: • Aria • AUDIX • CallPilot The default TUI is Aria.
Use Rapid Prompts	The option to define the default rapid prompts for users of a particular CoS. You can modify the mailboxes for users of a particular CoS without using the User Preferences page. The system displays the **Use Rapid Prompts** checkbox only when you install the rapid language pack on the AAM server.

Table continues…

Name	Description
Fax support	The fax feature for users who are assigned the class of service. The options to receive fax are: • **None**: Messaging disables the fax feature. • **Receive and forward to email**: Messaging forwards inbound faxes to the email address specified by the user in User Preferences. Messaging enables the outbound fax feature for the users. • **Detect and transfer to fax server**: The administered fax server receives inbound faxes. Messaging enables the outbound fax feature for users. If you do not configure Fax support on the Class of Service page, Messaging does not support fax transmissions for the users in the class. Messaging displays the correct fax receiving options in User Preferences. Messaging displays this option when the selected fax receiving method matches the method administered on the application servers where the users are registered.
Dial-out privilege	The types of calls that users in a class of service can make when using: • Call Sender • Play on Phone • Reach Me • Notify Me The valid values are: • **None** • **On Premise** • **Local** • **Long Distance** • **International**

Table continues…

Name	Description
User can use Reach Me	The Reach Me feature. For a new class of service, this check box is not selected by default. If you select the check box, the users who belong to the class can update the Reach Me page on the User Preferences page. If you change the value in the Dial-out privilege field to: • **None**: The system clears and disables this check box. • A value other than **None**: The system automatically enables this feature. **Note:** If you enable Reach Me feature for a mailbox, then the user cannot use the One-Step Recording feature. By enabling the Reach Me feature, you force callers to listen to the prompts.
Allow voice recognition for addressing (user can select recipients by saying their name)	The voice recognition feature for users to select recipients by saying the name of a recipient. For a new class of service, the check box is selected by default. If you clear the check box, the user cannot update the options in the **Voice Recognition for Addressing** section on the My Phone page in User Preferences.
Allow voice recognition for Auto Attendant	The feature by which the voice in speech enabled Auto Attendant selects users in a particular CoS. For a new class of service, the check box is selected by default.
IMAP4/POP3 access	The IMAP4/POP3 client to gain access to the message stores on an Avaya message store. The options are: • **Full** • **None** The default value is *Full*. **Note:** To increase the system capacity to either 30,000 or 40,000, you must disable the **IMAP4/POP3 access** feature.
Set Message Waiting Indicator (MWI) on user's desk phone	The indicator for a new message. For users who have a telephone with MWI, the indicator is lit when users receive a new message.

Table continues…

Name	Description
Enable password aging	The indicator for users to change their passwords periodically. If users do not change passwords within the specified time, the passwords expire and Messaging blocks the users until an administrator resets the passwords. Password aging is enabled by default. You can: • Set the password aging parameters on the System Administration webpage. • Reset expired passwords. Clear the **Voice messaging password expired** field on the User Managements webpage. **Note:** If you disable password aging for a particular class of service and again enable password aging: • The passwords of mailboxes that are older than the value that you administer in **Password Expiration Interval** on the System Administration page expire. • The status of the users in the group who were originally blocked because of an expired password is not reset. The users remain blocked from Messaging until you reset the password of the users.
Login Announcement recording	The permissions to administer the maximum length of login announcement that users can record in **Maximum length of login announcement** on the System Parameters page. The options are: • **None**: Users cannot record login announcement. • **Allow cluster level login announcement recording**: Users can record cluster-level login announcement. Messaging sends these login announcements to users in all sites administered in the application server cluster. • **Allow site level login announcement recording**: Users can record site-level login announcements. Messaging sends these login announcements to users in the sites administered on one application server. **Note:** MWI on the telephone does not light to indicate a new login message. **Note:** If you change the login announcement for a particular CoS, users logged in to Messaging Web Access must log in again for the change to take effect.

Table continues…

Name	Description
Address after message record	The option to add user addresses after recording the message. If you select this check box, users can record the message and then add the addresses of the recipients in the message. By default, this option is: • Selected for the Aria and Audix TUIs. • Cleared for the CallPilot TUI.
Allow auto login	The auto login feature for users. Users can automatically log in to their mailboxes without authentication. If you enable the auto login feature for the users of a specific CoS, the User Management webpage of the users display an **Auto Logon** check box. This check box is displayed for each extension administered for the users. Using these check boxes, you can enable or disable the auto login feature for each user extension. When you enable the auto login feature for an extension of a user, the user can enable or disable the auto login feature for each administered extension on the User Preferences page. This feature is disabled by default.
Allow users to block Call Answering (enable Message blocking options)	The feature to block incoming messages in User Preferences. If you select this check box, users can block incoming messages under specific conditions listed in **Messages blocking options**. **Note:** The **Messages blocking options** fields on the User Preferences page are only visible to users when you select this check box.
Allow addressing by number only	The feature to prevent users in a particular CoS from being listed in name search results. These users can only be found by their extension and mailbox numbers. If you select this check box, users composing and sending messages to these users can address them only by their number using TUI. When you select this option, you restrict these users from being addressed by name through Auto Attendant session transfers.
Allow Messaging Web Access	The feature to gain access and manage the voice mail messages using the secure Messaging web client. Messaging Web Access increases the processing load on the system even if users do not use the feature. Enable Messaging Web Access only for users who intend to use the feature. **Note:** To increase the system capacity to either 30,000 or 40,000 local users, you must disable the Messaging Web Access feature.

Table continues…

Name	Description
Save unsent messages if call dropped during recording	The feature to save unsent messages. If you enable this option, if a user loses connectivity to the telephony server while recording a voice message, the system automatically saves their work. For example, when a user is recording a message and call drops, the message is saved. When the user logs on to the Aria TUI next time, the user can access the saved message, do further recording, and then send the message. Unsent messages are saved in the Drafts folder in the mailbox on the Messaging storage server. This field is available for Aria TUI only.
Allow message deletion during playback	The feature to delete messages during playback. This field is available for Aria TUI only.
Mark a message as read	The feature to indicate when the system marks the message as read. The options are: • **When the user has played the entire message or interrupted playback after listening for at least 'X' seconds**: Configures the number of seconds that a message must be played before marking the message as read. • **Only when the user has played the entire message**: Marks a message as read after playing the entire message. This field is available for Aria TUI only.

Message Playback Options:

Using **Message Playback Options**, you can configure the default message playback order and the speed.

Users can override the settings for **Message Playback Options** using the User Preferences web interface.

Name	Description
Allow arrange messages by sender	This feature groups all messages from the same sender together. If the message does not include the name of the sender, Messaging sorts by the telephone number of the sender. If you select this check box on Class of Service page, Messaging displays the **Arrange by sender** option on the My Phone page in User Preferences.
Message playback order when the user reviews voice messages using the phone:	

Table continues…

Name	Description
For unread messages	The options are: • **Play newest first**: To hear messages starting with the newest first. • **Play oldest first**: To hear messages starting with the oldest message first. • **Play important messages before others**: To hear urgent messages first. • **Arrange by sender**: To hear messages that Messaging sorts by sender name. The system displays this option only when you select **Allow arrange messages by sender** option. This field is available for Aria and Audix TUIs.
For read messages	The options are: • **Play newest first**: To hear messages starting with the newest first. • **Play oldest first**: To hear messages starting with the oldest message first. • **Play important messages before others**: To hear urgent messages first. • **Arrange by sender**: To hear messages that Messaging sorts by sender name. The system displays this option only when you select **Allow arrange messages by sender** option. This field is available for Aria and Audix TUIs.
For saved messages	The options are: • **Play newest first**: To hear messages starting with the newest first. • **Play oldest first**: To hear messages starting with the oldest message first. • **Play important messages before others**: To hear urgent messages first. • **Arrange by sender**: To hear messages that Messaging sorts by sender name. The system displays this option only when you select **Allow arrange messages by sender** option. This field is available for Aria TUI only.

Table continues…

Name	Description
For all messages	The options are: • **Play newest first**: To hear messages starting with the newest first. • **Play oldest first**: To hear messages starting with the oldest message first. • **Play important messages before others**: To hear urgent messages first. • **Arrange by sender**: To hear messages that Messaging sorts by sender name. The system displays this option only when you select **Allow arrange messages by sender** option. This field is available for CallPilot TUI only.
Message playback speed level for playing back messages	The option to adjust the playback speed of your messages. The values of 'X' are 70%, 85%, 90% 100%, 125%, 170%.

Greetings:

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

Name	Description
None	The feature to disable the greeting. • If you select this option, you cannot select any options containing greetings in the **Block Message Delivery to Mailboxes when** filed on the System Administration page. SMI displays an error when you save the changes. • If you select an option containing greetings in **Block Message Delivery to Mailboxes when** before you administer CoS, SMI disables this option.
Personal internal and external greetings	The feature to enable only the internal and external greeting.
Personal and optional greetings	The feature to enable the personal and optional greetings instead of the personal internal and external greetings. Messaging plays the optional greeting according to the rules defined by a user on the Greetings tab on User Preferences.
Maximum length	The feature to administer maximum length of a greeting in seconds. The range of the recording that Messaging supports is from 5 to 300 seconds.

Table continues…

Name	Description
User can record extended absence greeting	The feature to record Extended Absence Greeting (EAG). Callers cannot dial-through an EAG. The system permits a fax transmission even if EAG is disabled for a user. The range of the recording that Messaging supports is from 5 to 90 seconds. When the timezones of the user and the Messaging system are different, upgrading the system from 6.3.1 to 6.3.3 and higher changes the expiration date and time of the extended absence greeting. The user must change the expiration date and time of the extended absence greeting after the upgrade.
Maximum length	The feature to administer maximum length of a greeting in seconds. The range of the recording that Messaging supports is from 5 to 90 seconds.
Block message recording if extended absence greeting is active	The feature to block callers from leaving a message if a user has activated EAG.
Play optional system greeting before user greeting	The feature to play an optional greeting before the following user greetings: • **Personal internal and external greetings** • **Personal and optional greetings** You can administer this greeting in the System greeting before the call answering field in the **Call Answering Greeting** section on the Sites page. You can use the optional greeting to play additional messages such as standard advertisements or disclaimers. **Important:** When you use the One-Step Recording feature, do not activate your system greeting. By activating the system greeting, you force callers to listen to the greeting.
Use specific call answer languages	The feature to use specific languages for call answering. If you select this check box, you can define specific languages for a particular CoS. If you clear this check box, Messaging uses the languages that are defined on the Sites page.
Default language	The list that displays the languages installed on the application server or the servers associated with a class of service. Use this option to select the default or the first language for a class of service. The default base language is English-US. The system uses the language that you select in this field to determine the language prompt that Messaging plays to callers who leave messages for all mailboxes within the site.

Table continues…

Name	Description
Additional language	The list that displays the languages installed on the application server or the servers that are associated with a class of service. Use the options to select two additional languages for a class of service. When you select an additional language, callers leaving messages for all mailboxes on this site receive a multilingual prompt.
Allow user to specify call answer languages	The feature to define specific languages for call answering on the User Preferences page. The **Use specific call answer languages** fields are only visible on the User Preferences page if you select this check box. Messaging disables this option for users if you install a bilingual language pack.

Notifications:

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

After you complete the information on the Class of Service webpage, users can gain access to User Preferences, enter the personal information on the General and Notify Me webpages, and begin using the Notify Me features that you enable.

Name	Description
Allow text message (or page) notification	The feature to send a text notification to a mobile phone or a pager to notify a user that the system delivered a new voice message to the mailbox of the user. For this: • The administrator must provide the email address of the appropriate SMS gateway. • Users must enable the Notify Me settings in User Preferences. Messaging supports only email-based SMTP pager and cellular notifications.
Allow outcalling notification	The feature to enable *outcalling*. *Outcalling* alerts a user to new messages with the system calling the user. *Outcalling* requires that users have the appropriate dial-out privileges.
Maximum number of rings	The maximum number of times that a designated outcall phone rings before the system hangs up during an outcall attempt. The valid range of values is from 1 to 10. This field is disabled if the Allow outcalling notification is set to No.

Table continues…

Name	Description
Start after	The delay between the time that a user receives a message and the first *outcall* attempt. The valid range is from 0 to 24 hours.
If no-answer or busy, retry after	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 delay between the time that the user receives the message and the system ends the outcall attempts. The range is 0 minutes to 24 hours.
Allow email notification	Messaging sends a text message to an email address to notify the user about a new voice message. The options are: • **Yes, with or without recording** • **Yes, only without recording** • **No** For this, users must enable the Notify Me settings in User Preferences. The system delivers email notifications in the .wav format.
Allow outbound fax email notification	The feature using which Messaging sends an email notification to the user when the fax is sent.
Enable read receipts for all composed messages	The feature that requests acknowledgement when the recipient has opened the mail.

Message Storage:

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

Name	Description
Maximum storage space	The maximum storage space allocated to a user. The range of the value is from 0 KB to 262,136 KB in multiples of 4 KB. You can set a minimum value of 4 KB and increase the value to 8 Kb, 12 KB, and 16 KB. If you increase or decrease the value by less than 4 KB, the value rounds down to the nearest multiple of 4 KB. For example, 27 KB rounds down to 24 KB. The default value is 16,800 KB.

Table continues…

Name	Description
Maximum call answer message length	The maximum duration of call answer messages that a user can receive. The range of the value is from 0 KB to 46,880 KB in multiples of 4 KB. You can set a minimum value of 4 KB and increase the value to 8 Kb, 12 KB, and 16 KB. If you increase or decrease the value by less than 4 KB, the value rounds off to the nearest figure with 0. For example, 23 KB rounds off to 20 KB. The default value is 2,400 KB.
Maximum voice mail message length	The maximum duration of voice mail messages that a user can compose. The range of the value is from 0 KB to 46,880 KB in multiples of 4 KB. You can set a minimum value of 4 KB and increase the value to 8 Kb, 12 KB, and 16 KB. If you increase or decrease the value by less than 4 KB, the value rounds off to the nearest figure with 0. For example, 23 KB rounds off to 20 KB. The default value is 2,400 KB. The value that you enter for voice mail messages indicates the size of a single message in KB. This value must not exceed the system value for the maximum message length.

Message Retention:

Using the Message Retention fields, you can control the period the system stores messages for the user.

After changing the **Message Retention** settings of a CoS in SMI, all logged in users of that CoS must log out of Messaging Web Access. Users must log in to Messaging again for the **Message Retention** settings to take place.

Name	Description
Unread messages in Inbox folder	The number of days that unread messages are stored in the Inbox folder. The options are: • **Forever**: Keeps messages forever. • **Warn after**: The warning period after which Messaging sends notifications that the messages in the mailbox have reached a maximum age. Messaging warns users before deleting the messages automatically. You can configure the **Warn after** option by entering the number of days in the **Warn after** field. For example, if you want messages to be deleted automatically after 30 days, then enter `30` in the **Delete After** field. To configure Messaging to warn users one week before the messages get deleted automatically, enter `23` in the **Warn After** field. Messaging alerts users that messages older than 23 days will be deleted. If users want to retain these messages, the users must take action. The **Warn After** period must be less than the **Delete After** period. When the user logs on to the TUI, the TUI warns the user with an alert. • **Delete after**: Keeps messages for a specified number of days. For example, if you enter 30 days, Messaging deletes messages that are over 30 days old. By default, Messaging deletes the messages after 45 days. The valid range of values is from 0 to 999.

Table continues…

Name	Description
Read messages in Inbox folder	The number of days that read messages are stored in the Inbox folder. The options are: • **Forever**: Keep messages forever. • **Warn after**: The warning period after which Messaging sends notifications that the messages in the mailbox have reached a maximum age. Messaging warns users before deleting the messages automatically. You can configure the **Warn after** option by entering the number of days in the **Warn after** field. For example, if you want messages to be deleted automatically after 30 days, then enter `30` in the **Delete After** field. To configure Messaging to warn users one week before the messages get deleted automatically, enter `23` in the **Warn After** field. Messaging alerts users that messages older than 23 days will be deleted. If users want to retain these messages, the users must take action. The **Warn After** period must be less than the **Delete After** period. When the user logs on to the TUI, the TUI warns the user with an alert. • **Delete after**: Keeps messages for a specified number of days. For example, if you enter 30 days, Messaging deletes messages that are over 30 days old. By default, Messaging deletes the messages after 45 days. The valid range of values is from 0 to 999.
Messages in other folders	The additional folders that users with IMAP access to the mailbox can create in the mailbox. This setting controls the number of days that messages are stored in the folders that users create. The options are: • **Forever**: Keeps messages forever. • **Delete after**: Keeps messages for a specified number of days. For example, if you enter 30 days, Messaging deletes messages that are older than 30 days. By default, Messaging deletes the messages that are older than 45 days. The valid range of values is from 0 to 999 days. This condition applies to the Drafts folders where unsent messages are stored.
Message restore allowed	The feature to restore messages that are marked for automatic deletion. When you select the check box, user gets an automatic deletion notification. The user can save or restore messages before Messaging automatically deletes the messages.

Related links

System Parameters field descriptions on page 178
Setting Messaging parameters on page 158
Changing user properties on page 191
Adding mobile operators on page 231
Basic and Mainstream mailbox licensing on page 215
Enhanced-List Application overview on page 236
Implementing ELA on page 236

Adding mobile operators

About this task

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, 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.
5. Click **Save**.

   The system saves the mobile definitions.

Next steps

Test the mail gateway for each mobile operator that you plan to support.

Related links

Testing mail gateways on page 232
Mobile Operators field descriptions on page 232

Testing mail gateways

Before you begin

- Add mobile operators.
- Provide a test phone or pager for each mobile operator that you add to the Mobile Operators webpage. 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, 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 231.
4. In the **Test** area, enter the appropriate information in the fields.
5. Click **Send**.
6. Validate that the mobile device received the test message.

Related links

Adding mobile operators on page 231
Mobile Operators field descriptions on page 232

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.

Table continues…

Name	Description
Address template	The identical part of the email address that the operator uses for all users. The system substitutes *{n}*, where *{n}* is the required number of digits for the appropriate mobile provider, with the number for the user. *{0}* denotes an unlimited number of digits. 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 before the number, add the prefix in the before the *{n}* variable. For example, the *9{10}@mobile.provider.com* address template corresponds to the *1234567890* phone number and does not correspond to the *11234567890* phone number.
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 that you want to test. The drop-down list displays the name in the **Description** field.
Message	The text that you want to send to your test device.

Deleting login announcement

About this task

Login announcements are active until you delete the message or record a new login announcement. You can also delete login announcements by clearing the ADCS cache.

If you select **Allow cluster level login announcement recording** or **Allow site level login announcement recording** from the **Login announcement recording** drop-down list on the Class of Service webpage, users can send login announcements using the TUI.

Before you begin

Ensure that the mailbox has privileges to send login announcements.

Procedure

1. Log in to the mailbox.

   You hear the following system prompt as part of the prompt for the mailbox main menu for the English-US language: `For login announcement, press 9.`

   If you use the CallPilot TUI, the system prompts you to press 5.

2. Press **9**.

   If there is a login announcement, you hear the following system prompt: `To review the login announcement, press 1. To record a message, press 2. To erase the login announcement, press 3.`

   If there is no login announcement, you hear the following system prompt: `There is currently no login announcement. To record a message, press 2.`

3. To delete the login announcement, press **3**.

Related links

Reloading application server cache on page 296

Login Announcements

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

Guidelines for Login Announcements

Login Announcements have the following characteristics. They:

- Do not turn message-waiting indicators. Hence, do not use login announcements for emergencies.
- Are not put in the mailboxes of the users. Users cannot delete, save, replay, or forward login announcements. To replay login announcements, user has to login again.
- They can be active only one at a time.
- Are delivered to users at remote locations
- Do not activate outcalling.
- Do not show up on TeleTypewriter (TTY) systems. Hence, a hearing-impaired user who uses only TTY for messaging does not see them. Send TTY users a mail message from a TTY.
- Go to all users of the system. Be sure to record all login announcements in all languages used.

Marking a message as a login announcement

About this task

Broadcast messages are now known as login announcements. You can record and send login announcement by pressing the appropriate keys.

Procedure

1. Log in to your mailbox.

2. To record a message using:
   - the Aria TUI, refer to *Avaya Aura® Messagin Aria Quick Reference*.
   - the Audix TUI, refer to *Avaya Aura® Messaging Audix Quick Reference*.
   - the CAllPilot TUI, refer to *Avaya Aura® Messaging CallPilot Quick Reference*.

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.

Note:

AAM 6.3.3 does not support the **User can send to system distribution lists (ELAs)** feature.

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.

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 webpage, click **Create a New List**.
3. Enter the appropriate information in the fields.
4. Click **Save**.

   The system saves the changes.

Next steps

Configure the External Hosts and Mail Options.

Related links

Changing external SMTP hosts on page 186
Configuring the mail options on page 393
Create a New Enhanced-List field descriptions on page 238

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.
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.
***PIN**	The password for the Enhanced-List mailbox. Passwords must follow the complexity rules for subscriber mailbox. For more information, see *Password complexity enhancement for Subscriber mailbox*. 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 50-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. You must not assign the mailbox number to another local user. On a multisite system, the user mailbox can be of any length between 3 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. 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**	The CoS for ELA is *8–ELA*.
***Community ID**	Do not change this field. Use the feature to allow or deny voice mail among different communities.
Messaging Locale	The language of the Messaging system.

ENHANCED-LIST FEATURES

Name	Description
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?	Specifies the system allows to broadcast messages to all local subscribers. The options are: • **off**: Sends ELA messages only to the list members that you specify on the Manage Enhanced-List webpage. • **as broadcast message**: Sends the message to all users of a system. If the user is a member of the ELA list, the user will receive duplicate message, one as a normal message and one as a broadcast message. **Note:** The system displays the **as broadcast message** option, only when you configure **Broadcast Mailbox Number** on the System Mailboxes webpage. The system sends all broadcast messages as priority messages. Unheard broadcast messages do not take up space in a recipient mailbox.
Light MWI for Broadcast Messages?	The option to administer the MWI light for broadcast messages. The default is *no*. **Note:** When you send a broadcast message, the MWI lamp is not lit immediately, but may lit later after scanning the mailbox and leaving the broadcast message in an unseen state.

SUBSCRIBER DIRECTORY

Name	Description
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* .

Table continues…

Name	Description
Telephone Number	The telephone number of the list. This number must be in the same format as 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. 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

Name	Description
Immediately Expire Password?	The feature 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. To prevent unauthorized access to the mailbox, add an extra layer of protection by selecting *yes* to lock the mailbox. Add an extra layer of protection by selecting *yes* to lock the mailbox because of unsuccessful login attempts and prevent access to the mailbox.

MAILBOX FEATURES

Name	Description
Voice Mail Enabled	The option to enable **Voice Mail** feature for a mailbox.

MISCELLANEOUS

Name	Description
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 webpage to load the following lists:

- User List
- Global Address List

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.

   The system displays the Operation in progress dialog box. When the system completes the reload operation, the dialog box does not show.

Administering an ELA List

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

Procedure

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Enhanced List Management**.
2. On the Manage Enhanced-Lists webpage, you can click on the respective buttons to:
   - Sort the lists.
   - Display a report of all the lists.
   - Create a new list.
   - 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.

Related links

Adding a new ELA list on page 237

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.
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 5: 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

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.

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.

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

Name	Description
List Name	The name of the enhanced list.

Table continues…

Name	Description
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 that you back up the message store.

Caller Application contains three types of information:

- Application management data
- Application structure
- Application prompts

Application prompts occupy the largest amount of space.

The maximum size of a Caller Application must be equal to or higher than the amount of space that the application prompts occupy.

Important:

Caller applications require all servers to run the same Messaging release. Running different Messaging releases in servers might affect the functioning of some features.

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 get information about MMC through the MMC Help menu.

Note:

Set the DPI scaling size to 100% for correct display of Caller Applications Editor User Interface in Windows 7.

System requirements

- A computer that is running one of the following operating systems:
  - Windows Server 2003
  - Windows Server 2008
  - Windows Vista
  - Windows 7 32–bit
  - Windows 7 64–bit
  - Windows 8.1 32–bit
  - Windows 8.1 64–bit
  - Windows 10 32–bit
  - Windows 10 64–bit
- The following software from the Microsoft Download Center:
  - MMC 3.0
  - .NET Framework 3.5, 4.5, and later.
- 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 following:

- 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.
- Class of Service
- Language
- Site
- The caller menu logic.

For more information, see:

- Worksheet for container properties on page 254.
- New Caller Application field descriptions on page 263.

Prompts

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

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

Recording an audio prompt

About this task

The Caller Applications Editor GUI is available only in English-US, but you can record prompts in any language.

Procedure

1. Open the application that you use to record `.wav` files.
2. Set the recording parameters according to the following Avaya Aura® Messaging requirements for `.wav` files:

   8,000 Hz/8–bit mono, mu-law.

   Note:

   If you use other parameters, Avaya Aura® Messaging might experience issues when playing this audio prompt.
3. Speak into a microphone that is connected to the computer, and record the greeting.
4. Assign a name to the `.wav` file.
5. Play the greetings on the computer to assure it is accurate and audibly acceptable.

6. Using the Caller Applications Editor, upload the `.wav` file.

Adding prompt to caller application

About this task

The `.wav` file requires the 8,000 Hz/8-bit mono mu-law format. 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. Use this procedure only when the encoding is correct.

Procedure

1. In the Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. In the Name pane, right-click the caller application and select **Properties**.
3. Select the **Prompts** tab and click **Add**.
4. Navigate to the folder that contains the `.wav` file.
5. Select the `.wav` file and click **Open** to upload it.

   If the encoding is incorrect, use an application to create a file with the correct encoding.

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 configure the type of action for each key.

Action	Description
Auto Attendant	Forwards the call to the Auto Attendant so the caller can dial by entering an extension number on the keypad, by entering the name of the mailbox, or by saying the name of the mailbox.
Go to mailbox number	Transfers the call to the mailbox specified in **Mailbox number**, such as a nonbusiness hours mailbox. If you also select **Non-specified mailbox number**, Messaging prompts the caller to enter a mailbox number. **Important:** For this option to work correctly, the caller must ensure that the delay between entering each digit of the extension number must not exceed 2 seconds.
Transfer to extension	Transfers the call to the extension that the caller enters. If you also select **Non-specified extension**, Messaging prompts the caller to enter a number. If you select **Extension** and enter the extension or mobile phone number, the owner of the number can dial `#3` and record or change the **Instructions** prompt. The transfer to the extension or mobile phone number which does not have a mailbox associated with the number work only if the administrator enables the **Allow transfer to non-native mailbox extensions** in site. **Important:** For this option to work correctly, the caller must ensure that the delay between entering each digit of the extension number must not exceed 2 seconds. **Security alert:** If your network is not properly secured, activating the option for callers to enter a mailbox or an extension number increases the risk of toll fraud.
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.

Table continues…

Action	Description
Hang up	Ends the call.
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** Use Text to Speech to say: *Hello, Welcome to the ABC store.*	**Continue menu** Play the Instructions prompt.
Allow enter number for	Allows a caller to enter the mailbox or extension number and, depending on the administration, transfers the call. The options are: • **Go to mailbox number** • **Transfer to extension** **Important:** For this option to work correctly, the caller must ensure that the delay between entering each digit of the extension number must not exceed 2 seconds. **Security alert:** If your network is not properly secured, activating the option for callers to enter a mailbox or an extension number increases the risk of toll fraud.	—

Table continues…

	Change action or select the prompt dialog	
Menu action	**First perform this action:**	**Then perform this action:**
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.	—

Table continues…

	Change action or select the prompt dialog	
Menu action	**First perform this action:**	**Then perform this action:**
Key 6	**Transfer to extension** 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

Plan the basic properties for the caller application container and the 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.

Perform the first two tasks in sequence and the other tasks in any order.

No.	Task	References	✔
1	Create a plan for the caller menus and the prompts.	• Worksheet for container properties on page 254 • Worksheet for menus on page 255	
2	Define a caller application container.	Creating containers on page 263	
3	Define the schedule for each caller menu.	• Creating business schedules on page 266 • Creating holiday schedules on page 266	
4	Create the call menus.	Creating menus on page 265	
5	Load audio prompts.	Assigning audio prompts to menus on page 267	

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	Value
Name of the caller application	
Mailbox number	Test: Production:
Extension	Test: Production:
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* 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: _____ • Continue menu		
Allow enter number for	• Go to mailbox number • Transfer to extension		
Instructions	• Play audio file from Prompts list • Use Text-to-Speech to say		

Table continues…

		Complete only for Play Prompt actions	
Prompt or key press	**Menu action (select one)**	**Filename or TTS text**	**Define next action**
Key 1	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default) • Continue menu		
Key 2	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default) • Continue menu		

Table continues…

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

Table continues…

		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) • Continue menu		
Key 6	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default) • Continue menu		

Table continues…

		Complete only for Play Prompt actions	
Prompt or key press	**Menu action (select one)**	**Filename or TTS text**	**Define next action**
Key 7	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default) • Continue menu		
Key 8	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default) • Continue menu		

Table continues…

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

Installing Caller Applications Editor

Procedure

1. In your browser, type the following URL: `https://<IP address or FQDN of the Messaging storage server>/download/CallerApplicationsEditor.msi`.

   Messaging displays the File Download dialog box.

2. Click **Run** and follow the instructions in the Avaya® Aura Messaging Caller Applications Editor Setup wizard.

3. In the Destination Folder dialog box, do the following:
   - **Create a Desktop icon**: To create a shortcut for launching the Caller Applications Editor on the desktop, select the **Create a Desktop icon** check box. This check box is unchecked by default.
   - **Create Start Menu entry**: To create a shortcut to **All Programs** under **Start** menu, select the **Create Start Menu entry** check box. This check box is checked by default.
4. On the Completed the Avaya® Aura Messaging Caller Applications setup wizard, select the **Launch Caller Applications Editor** check box.
5. Click **Finish**.

Note:

The install file or application file does not have the current versioning and does not recognize the newer version of Caller Application Editor (CAE). Hence, you must uninstall the older version before installing the newer version of CAE.

Related links

Installing Caller Applications Editor in the silent mode on page 261

Installing Caller Applications Editor in the silent mode

About this task

Use this procedure to do the automated installation of the Caller Applications Editor for a large number of users. Installing the Caller Applications Editor automatically does not require user interaction and does not display messages or prompts.

Procedure

1. Start the program from the **Start** menu.
2. In the **Run** window, type `cmd`.
3. On the command line interface, type the following: `msiexec /I CallerApplicationsEditor.msi /quiet ADDDESKTOPICON=1 ADDSTARTMENUICON=1 RUNAPPAFTERINSTALL=1 where:`
   - ADDDESKTOPICON=1: Adds a shortcut to the desktop.
   - ADDSTARTMENUICON=1: Adds a shortcut to the menu.
   - RUNAPPAFTERINSTALL=1: Launches the application automatically.

Changing the Caller Applications password

About this task

Use this procedure 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, type the new password in the **Password** field.

   Some browsers automatically populate web-based forms with passwords. If **Password** contains a value, clear the field and enter the password. To prevent Messaging from automatically populating the passwords, turn off the option to remember the password in your browser.
3. Type the password in the **Confirm password** field.
4. Click **Save**.

   The system saves the settings.

Related links

System Policies field descriptions on page 199

Working in Caller Applications Editor

Logging in to Caller Applications Editor

Before you begin

- All required software is loaded on your computer.
- Note the IP address or FQDN of the storage server.
- Note the password for Caller Applications Editor. The default password is `caadmin01`.

Procedure

1. Click **Start** > **All Programs** > **Avaya Connector** > **Avaya AxC CallerApps**.

   The system displays the Connect to Messaging AxC window.
2. Enter the following information in the fields:
   - **AxC address**: The IP address or FQDN of the storage server.

- **Password**: The password for Caller Applications Editor.

3. Click **OK**.

Note:

If you upgrade or migrate to Avaya Aura® Messaging 7.1.0 from Releases prior to 6.3.3, you must save Caller applications using the latest release of Caller Applications Editor after migration.

Caller Applications Editor displays the IP address of the AxC connector in the title bar and the navigation pane.

Related links

System requirements on page 247

Creating containers

Procedure

1. In Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. Right-click **Caller Applications**.
3. Select **New** > **Caller Application**.
4. Enter the appropriate information in the **New Caller Application** dialog box.
5. Click **OK**.

   The system creates the caller application.

Next steps

Create menus.

Related links

Creating menus on page 265
New Caller Application field descriptions on page 263

New Caller Application field descriptions

Name	Description
Name	The name of the caller application.
Mailbox number	The mailbox number for the user account of the caller application. All mailbox numbers for user accounts must be unique. However, the mailbox number does not have to match the extension.

Table continues…

Name	Description
Include in Auto Attendant Directory	The option to make the caller application accessible through the Auto Attendant directory. If you select **yes**, complete the **Pronounceable name** field if the spelling of the name is different from the pronunciation.
Extension	The numbers 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. Use additional extensions when: • Multiple DID numbers access the caller application. • A caller application migrates from a legacy phone system, and the internal 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.
Class of service	The CoS of the new caller application. You can define the maximum size of caller applications in the **Maximum voice mail message length** field in the **Message Storage** settings on the Class of Service page. The value of voice mail messages specifies the size of a single message in KB. This value must not exceed the system value for the maximum message length.

Table continues…

Name	Description
Pronounceable name	The user name spelled according to the pronunciation. If a user or info mailbox has a name that you can pronounce in different ways, spell the name as you pronounce the name. For example, spell Dan DuBois as `Dan Doobwah`. This entry reduces the number of attempts that the Speech Recognition feature makes to match a spoken name with the name in the Auto Attendant directory. You can also enter an alternative name. For example, if the original name of the caller application is *Customer Support*, you can enter *Technical Support* in the field. The speech engine then recognizes both the names.
Language	The language configured for caller applications. The administrator can configure any one language from the list of installed languages. This configured language is used for call transfers. The language installed for a caller application can differ from a site language.

Creating menus

Before you begin

Create a container for the caller application.

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 267.
6. Click **OK**.

   The system creates the menu.

Related links

Creating containers on page 263
Assigning audio prompts to menus on page 267

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 recorded audio prompts.

   For information about recording audio prompts, see *Recording an audio prompt*.
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.

   Repeat these steps for each additional caller application.

Related links

Menu actions on page 250

Deploying a caller application

Before you begin

- Create and test the caller application.

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 **OK**.

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

Related links

Loading lists on page 146

Allowing callers to enter a number to transfer a call

Security alert:

If your network is not properly secured, allowing callers to enter a mailbox number or an extension, increases the risk of toll fraud.

About this task

With the **Allow enter number for** option, you can administer an option for callers to manually enter an extension number or a mailbox number to transfer their call.

Procedure

1. In Caller Applications Editor, expand the **Caller Applications Editor**.
2. Select one of the following **Properties** tab for the menu that you want to create:
   - **Business Hours Menu**
   - **Off Hours Menu**
   - **Holiday Menu**
3. On the selected tab, click **Change** next to **On Answer**.

   Caller Applications Editor opens the Change Action window.
4. From the **On Answer**, select **Play Prompt**, and click **Continue menu**.
5. Select the **Allow enter number for** check box.
6. From the **Allow enter number for** list, select one of the following options:
   - **Transfer to extension**: Caller Applications Editor prompts callers to enter an extension number.
   - **Go to mailbox number**: Caller Applications Editor prompts callers to enter a mailbox number.
7. On the **Menu** section, create your customized menu.
8. Click **OK**.

Related links

Assigning audio prompts to menus on page 267
Creating menus on page 265
Recording and sending audio prompts on page 269

Importing TTY prompts

Recording and sending audio prompts

About this task

Import audio prompts as TTY prompts in Caller Applications Editor or use these audio prompts in the .wav format as Auto Attendant greetings. Using a TTY device, you can send audio prompts to your email inbox and get these .wav files through Microsoft Outlook.

Procedure

1. Using your TTY device, log in to Messaging.
2. To record a message, press the appropriate key on your TTY device.
3. When the TTY device displays the GA prompt, type a message, and press the Pound (#) key.

   You can use this message as a customized TTY prompt for Caller Applications Editor or as an Auto Attendant greeting.
4. Dial your mailbox number, and press the Pound (#) key.
5. To end the address, press the Pound (#) key again.
6. To send the recorded message, enter the appropriate combination of keys for your TUI.

   The system sends the message and displays the main menu. To record more messages, repeat Step 2 to Step 5.

Next steps

Get the audio prompts from your email inbox.

Related links

Assigning audio prompts to menus on page 267
Creating menus on page 265
Allowing callers to enter a number to transfer a call on page 268
Logging in to Messaging on page 37

Getting audio prompts using Microsoft Outlook

About this task

Import audio prompts as TTY prompts in Caller Applications Editor or use these audio prompts in the .wav format as Auto Attendant greetings. Using a TTY device, you can send audio prompts to your email inbox and get these .wav files using Microsoft Outlook.

Procedure

1. On the Microsoft Outlook menu, click **File** > **Info** > **Account Settings** > **Add Account**.

   Microsoft Outlook displays the Add New Account window.

2. Select **Manually configure server settings or additional server types**, and click **Next**.

   Microsoft Outlook displays the Choose Service window.

3. Select **Internet E-mail**, and click **Next**.

   Microsoft Outlook displays the Internet E-mail Settings window.

4. In the User Information section, type values for the following fields:
   - **Your name**
   - **E-mail address**
5. In the Server Information section, enter values for the following fields:
   - **Account type**: Select **IMAP**.
   - **Incoming mail server**: Type the Messaging server address which your system administrator provided.
   - **Outgoing mail server (SMTP)**: Type the Messaging server address provided by your system administrator. The outgoing mail server address must be identical to the incoming mail server address.
6. In the Logon Information section, enter values for the following fields:
   - **User Name**: Type the Messaging user name.
   - **Password**: Type the Messaging password.
7. Click **Next**.
8. Click **Finish**.
9. Check your email inbox for the email containing the .wav files of the recorded prompts, and save the .wav files on your local drive.

Next steps

- Import the audio prompts to TTY.
- Administer these audio prompts as Auto Attendant greetings.

Importing TTY prompts in Caller Applications Editor

Before you begin

Ensure that you have audio prompts to add to Caller Applications Editor in the .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 select **Properties**.
3. Select the **Prompts** tab, and click **Add**.
4. Select .wav file and click **Open**.

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.
- 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).

Related links

Ensure voice quality on page 273

Setting up a teletypewriter for your system and the user

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.

Do not configure:

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

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

Procedure

1. On the Languages webpage, install the *English (United States) - TTY* language pack.
2. On the Sites webpage, do the following:
   - In the **Main Properties** area, in the **Site Default Language** field, click **English (United States) – TTY** .
   - In the **Auto Attendant** area, in the **Default Language** field, click **English (United States) – TTY**.

   The system creates a new site for TTY users.
3. On the Miscellaneous webpage, set the audio encoding format to *G.711*.

   Do not enable G729 option. If, you enable the G729 option, users lose the texts on the TTY device.
4. In the **User Preferences** menu, instruct the users to select the language as **English (United States) - TTY**.

   The system defines the default language for user login sessions.

Related links

Configuring languages on page 115
Configuring the miscellaneous information on page 444
Speech recognition on page 192

Caring for your hearing-impaired users

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 TTY device* section in *Using Avaya Aura® Messaging*.

Ensure that teletypewriter users receive login announcements

The Messaging system sends login announcements 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

- Language packs

You must install the following patches when available:

- Security
- Kernel

For each type of service pack, when the latest version is available, you must install the service packs in the following order:

1. Kernel
2. Security
3. Communication Manager
4. Messaging
5. Language packs

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.

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.

Related links

Downloading service packs on page 275
Installing a service pack on page 276

Downloading service packs

Procedure

1. In 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 **Browse** 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 the complete URL of up to four files.
   b. 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 (:).
   c. Click **Download**.

Installing a service pack

Procedure

1. Log in to Messaging System Management Interface with the Customer Privileged Administrator account user and password created earlier.
2. Click **Server (Maintenance)** > **Server Upgrades** > **Manage Updates**.

   The Manage Updates page displays the list of uploaded service packs.
3. Select a service pack from the list.
   a. Click **Unpack**.
   b. Click **Continue** to return to the Manage Updates page.

   The status of the selected service pack changes to **unpacked**.
4. Select the same service pack from the list.
   a. Click **Activate**.

      If the service pack installation process affects the availability of the Messaging service, the system prompts you to confirm the action.
   b. **(Optional)** Click **Yes** to confirm the action.
   c. Click **Continue** to return to the Manage Updates page.

   The status of the selected service pack changes to **activated**. If the selected service pack is a kernel service pack, the status stays in the **activating** state until about one minute after the system reboots. Then the status changes to **pending_commit**.

   Note:

   The service pack installation process takes approximately 10 minutes for a kernel or security service pack.
5. Click **Messaging** > **Server Information** > **System Status** to verify that the Messaging system is functional.

The System Status webpage displays the status of the various processes and modules depending on the server role.

Server role	Status of the processes and modules	Examples
Application only	All entries in the list of processes must have a status of `Running` or `Online`, which is displayed in green.	• Voice Messaging Application - Last known AxC status • Voice Browser • Speech Server • User Data Migration • Application Distributed Cache Server • Storage Synchronizer • Web Access - Java Servlet Container (Tomcat) - HTTP Server (Apache)
Storage only	All entries in the list of modules must have a status of `IN SERVICE` or `UP`.	• Message Store • Other enabled software modules such as: - Enhanced-List Administration - Internet Messaging - LDAP processes - Corporate LAN LDAP Access - Voice System
Application and storage	All entries related to the lists of processes and modules must have the respective status.	Both of the above.

Tip:

Click the **Refresh** button of your browser until all entries show the relevant status.

Note:

The system reboots for a kernel or security service pack installation. During the system reboot, the System Status webpage remains inaccessible.

6. Verify that the status of the installed service pack shows **activated** on the Manage Updates page.

7. **(Optional)** If the status shows **pending_commit**, select the service pack from the list.
   a. Click **Commit**.

b. Click **Yes** to confirm the action.

c. Click **Continue** to return to the Manage Updates page.

Installing software

The software installation page displays the packages available for installation.

Before you begin

Use a privileged administrator account with the necessary rights and do the following steps:

- Create a privileged administrator login.
- 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.
- 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.
2. On the **Administration** menu, click **Messaging** > **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system lists all 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.

Messaging performs a series of background checks on the system software. Messaging checks the content of each installed executable or help file, but not data files, to verify that the files are unchanged since the system installation or update. Depending on the system configuration, it might take several minutes to display the report.

Note:

The configuration files constantly change and are unlikely to verify successfully.

The report includes each of the primary software packages installed on the system. Exceptions are marked with attribute flags. These attribute flags only appear for problem files. Messaging displays `Missing` for a file that is removed from the expected directory.

The report listings are formatted as:

```
SM5DLUGT c <file>
```

Where SM5DLUGT c are the possible attribute flags and is the name of the file that fails verification. If no problem has been found for a certain attribute, Messaging displays a period (.) as a placeholder.

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.

Example

The following example indicates that the file size and modification time of the banner.dat file are different from the original file installed:

```
S......T /html/base/config/banner.dat
```

Where:

S	Designates the file size.
M	Designates the file mode.
5	Designates the MD5 checksum of the file.
D	Designates the major and minor numbers of the file.
L	Designates the symbolic link contents of the file.
U	Designates the owner of the file.
G	Designates the group of the file.
T	Designates the modification time of the file.
c	Appears only if the file is a configuration file.
<file>	Represents the name of the file, along with the file path, that fails verification.

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.

- Create a privileged administrator login.
- 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.
- 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**.

Related links

Adding a privileged administrator login on page 33
Adding a Web Access Mask on page 415

Deleting software packages

Before you begin

You must perform the following steps using a privileged administrator account with the necessary rights.

- Create a privileged administrator login.
- 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.

- 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.

Related links

Adding a privileged administrator login on page 33
Adding a Web Access Mask on page 415

Chapter 14: Back up and restore

Backup and restore overview

Purpose of backup and restore

Messaging uses LAN to back up the Messaging data to an external server. You can back up the Messaging application data and the server data simultaneously or independently. During a system failure, Messaging uses the information stored on the external server to restore the system. Messaging supports up to 40,000 mailboxes. A Messaging data backup can exceed 50 GB. Customers might be unable to support transfers of a single file of this size. Hence, Messaging automatically divides large data backups into 500 MB files before the file transfer. If a file transfer exceeds 5 minutes for each 500 MB file, Messaging considers the longer period as a backup failure and ends the backup. To ensure that the files transfer within 5 minutes, the network must support a minimum average transfer rate of 25 Mbps. Messaging supports the following backup methods:

- SFTP
- SCP

Note:

When the backup of server data and Messaging application data to the SFTP server is complete, ensure that the backup files are transferred successfully to the SFTP server.

While administering network backups using SCP or SFTP, ensure that you know the possible file storage sizes and the limitations of the storage size on the customer data network.

You can limit 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 that a message can remain in a mailbox before the system deletes the message. The system default is 45 days after which 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 manually back up any combination of the following Messaging data types using **Backup Now** or automatically according to a schedule using **Scheduled Backup**. The data types are:

- Translations
- Messaging names
- Messaging application and messages

Note:

The system does not include language packs and login announcements in the backup. Ensure that you install language packs on each application server.

Translations

Translations include data administered on the following SMI webpages:

- System Administration
- Telephony Integration
- Telephony Domains
- External Hosts
- Enhanced List Management
- Users
- Class of Service
- IMAP Traffic

Besides scheduled backups, you can also perform backups when you make extensive changes to user profiles.

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:

- Primary voice greeting
- Multiple personal greetings
- Automated attendant menus
- Messages

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** webpage to restore backed-up system files.

Restore backups when an alarm repair action prompts you.

Backup verification

You must verify the success of each backup that you run. A backup can include many data types, in addition to Messaging server data. The View Backup Log screen, which is available from the Server (Maintenance) webpage, 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 data that you selected to back up.

If you perform backup and restore on the storage server, the Sites webpage data or provisioning data that the storage server uses is different than the data 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 webpage data in the cache that the application server maintains.

Backing up the system

About this task

Messaging uses LAN to back up the Messaging data to an external server. The Messaging application data and the server data can be backed up simultaneously or independently. During a system failure, Messaging uses the information stored on the external server to restore the system.

Messaging supports the following backup methods:

- SFTP
- SCP

Procedure

1. Log in to Messaging System Management Interface.
2. In the **Administration** menu, click **Messaging** > **Utilities** > **Stop Messaging**.
3. Click **Stop**.

   The system delays the shutdown for three minutes after which the system ends all active calls.

   The Stop Messaging Software webpage refreshes periodically during the shutdown routine. After the Messaging software stops, the system displays the `Stop of Messaging completed` message.
4. Click **OK**.
5. In the **Administration** menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Backup Now**.
6. On the Backup Now webpage, in the **Data Sets** area, select **Full Backup** option.

   The system takes a backup of the **Server and System** files and **Security** files.
7. In the **Backup Method** area, click **Network Device** and then complete the following fields:
   a. **Method**

b. **User Name**
c. **Password**
d. **Host Name**
e. **Directory**

8. **(Optional)** If you want to encrypt the backup data, select **Encrypt backup using pass phrase** and enter a pass phrase using an arbitrary string of 15 to 256 characters.
9. Click **Start Backup**.

   For more information, see Backup Now field descriptions on page 285.

   Note:

   - Before you start Messaging, wait for the backup to be complete. When the backup is complete, the system displays the message `Backup successfully completed`
   - When the backup of server data and Messaging application data to the SFTP server is complete, ensure that the backup files are transferred successfully to the SFTP server.

10. In the **Administration** menu, click **Messaging** > **Utilities** > **Start Messaging**.

    The Start Messaging Software webpage is refreshed periodically during the startup process and displays a status message after displaying the **Start Messaging information** message.

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

11. Click **OK**.

Backup Now field descriptions

Name	Description
Data Sets	

Table continues…

Name	Description
Specify Data Sets	The data sets that you want to back up. The 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**
Full Backup	A full backup that 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 methods available for backup. The options are: • **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. • **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 IP address of the SCP or SFTP server on which the data has been backed up.
Directory	The network directory on which the backup is stored.
Encryption	
Encrypt backup using pass phrase	The option 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 Messaging data

About this task

If your Messaging topology contains more than one application role for a specific site, configure all application roles that support the site identically. To ensure identical configuration, back up the application files of the first server to other application servers.

If your topology contains multiple sites, note that the sites have different settings, such as different dial plans. Do not restore backed-up files from one site onto servers that support a different site.

The time taken to back up the application files depends on the amount of data.

Before you begin

- Get the login credentials to a file transfer server, which uses SFTP or SCP, for storing the Messaging backup data.
- Complete all administration tasks for the first application role.
- Ensure that Messaging is not running.

Procedure

1. In the **Administration** menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Backup Now**.

   Messaging displays the Backup Now webpage.

2. In the **Data Sets** area, select **Specify Data Sets**.
3. Select the **Messaging** check box, and then select **Messaging Application**, **Translations**, **Names** and **Messages**.
4. In the **Backup Method** area, select **Network Device**, and choose a location for the backed-up files in the following fields:
   - **Method**: Select SCP or SFTP.
   - **User Name**
   - **Password**
   - **Host Name**: Enter the IP address.
   - **Directory**: Enter the full directory path to store the backup.

   Note that you need this information to restore the data onto other servers.

   Note:

   When the backup of server data and Messaging application data to the SFTP server is complete, ensure that the backup files are transferred successfully to the SFTP server.

5. Click **Start Backup**.

   Messaging starts the data backup.

6. Start Messaging.

Next steps

Restore the backed-up data set on to all additional application servers for the site.

Related links

Stopping Messaging on page 460
Starting Messaging on page 460
Backup Now field descriptions on page 285

Restoring application files

About this task

If your Messaging topology contains more than one application role for a specific site, configure all application roles that support the site identically. To ensure identical configuration, back up the application files of the first server to other application servers.

If your topology contains multiple sites, note that the sites have different settings, such as different dial plans. Do not restore backed-up files from one site onto servers that support a different site.

The time taken for to restore the application files depends on the amount of data.

Before you begin

- Integrate the application server for a site with your telephony server.
- Ensure that you have the information that you entered on the Backup Now webpage.
- 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. Start Messaging.

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.
- Validate your Messaging configuration.

Related links

Starting Messaging on page 460
Initial administration checklist for sites and topology on page 120
Messaging configuration checklist on page 147

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. You might even 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.

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, so that the Messaging server can handle breaks in the LAN connection and create a successful backup. To run a scheduled backup that failed, schedule the backup to run on the current day and 5 or 10 minutes in the future.

Related links

Adding a new backup schedule on page 289

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** for a single server or a storage server.
   - **Messaging Application and Translations** for an application server.
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

About this task

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 how the system recorded the data. Use the Backup Logs webpage 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 webpage, 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 webpage.
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.

System restore checklist

Use this checklist as a guideline for the sequence of tasks to restore the system.

No	Task	Reference	Note
1	Restore the data from the backup.	Restoring data on page 294	—
2	Verify the server roles and the AxC address.	Administering the server role and AxC IP address on page 42	If you change the server roles, you must restart Messaging and log in to SMI again. If you change the AxC IP address, ensure that the server at the IP address that you administer is an operational storage and AxC server.
3	Verify the topology and check that the correct application servers are listed.	Adding additional application servers on page 132	Perform this task only for a storage server or a combined application and storage server.
4	Verify the topology and check that the sites are active on the correct servers.	Activating sites on page 52	Perform this task only for a storage server or a combined application and storage server.
5	Verify the cluster configuration	Configuring a cluster on page 110	Perform this task only for an application server or a combined application and storage server if you configured a cluster in your network. • To change the configuration of the cluster, see Changing the configuration of a cluster on page 184. • To run diagnostic tests to verify the connectivity and the cluster configuration, see Running application server diagnostics on page 422
6	Update the subscriber data on the remote servers.	Running a remote update manually on page 211	Perform this task only if your network has remote servers.
7	Manually synchronize the ADCS cache.	Synchronizing the ADCS cache on page 296	Perform this task only for an application server or a combined application and storage server.

Restoring data

About this task

The time required to restore the database depends on the amount of data in the backup and the LAN speed. Do the following procedure for attended and unattended backups.

Procedure

1. In the **Administration** menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **View/Restore Data**.

   The system displays the View/Restore Data webpage.

2. In the **View current backup contents in** area, select **Network Device** or **Local Directory**.
3. If you select **Network Device**, in the following fields, enter the same information that you used when you backed up the data:

   - **Method**
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

   In **Host Name**, enter the IP address of the backup server.

4. If you select **Local Directory**, enter the path of the directory.
5. Click **View**.

   If you do not select a backup image, the system displays an error message. To clear the error message, click **Back** on the browser and then select a backup image.

6. On the View/Restore Data Results webpage, select a backup image stored in the location that you specified.

   The system lists the most recent backups at the bottom of the list.

7. To select the backup image you want to view or restore, click the corresponding option.

   If the server name does not match or if you are performing a server migration procedure, click **Force Restore if server name mismatch or server migration**.

   If you want to restore both the Messaging server data sets and the Messaging data sets, you must first restore the Messaging server data.

8. Click **Preview** if you are unsure that you selected the correct backup image.

   The system displays a brief description of the data associated with the backup image.

Full Backup files and Messaging data files have names attached to the backup file names. When we select **Full Backup**, the system creates Full Backup files that include server files, system files and security data sets. The following name is attached to the backup file name:

- full-*

For Messaging data files that include Messaging Application, Translations, Names and Messages, the following names are attached to the backup file names:

- audix-ap-tr-msg-* for translations, messages, and messaging applications
- audix-ap-tr-name-msg-* for translations, names, messages, and messaging applications
- audix-ap-tr-name-* for translations, names, and messaging applications
- audix-ap-tr-* for translations and messaging applications only

9. Click **Restore** on the second screen to begin the restore process.

   If the server name does not match or if you are performing a server migration procedure, click **Force Restore if server name mismatch or server migration**.

   When you click **Restore**, the system displays the View/Restore Data Results webpage with the status of the restore process.

   Note:

   For restoring data fully, do the following:

   - Restore Full Backup that was backed up. For more information, see Backing up the system on page 284.
     - Perform *Restoring data* procedure with full-* for server files, system files and security files.
   - Restore Messaging data that was backed up. For more information, see Backing up Messaging data on page 287.
     - Perform *Restoring data* procedure with audix-ap-tr-name-msg-* for translations, names, messages, and Messaging application files.

Related links

Stopping Messaging on page 460
Starting Messaging on page 460
Reloading application server cache on page 296

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** • **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.

Reloading application server cache

About this task

Use this procedure to manually reload cache on each server with application role after you restore the database.

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.
4. To reload User List, click **Reload**.
5. To reload Global Address List, click **Reload**.
6. To synchronize ADCS, click **Synchronize**.

Related links

Stopping Messaging on page 460
Starting Messaging on page 460

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.

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

About this task

Use the Current Alarms webpage 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

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.
Major	The alarm is a major alarm.
ID	A unique identification number assigned to the alarm.
APP	The name of the application.

Table continues…

Name	Description
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

About this task

The Certificate Alarms webpage 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 webpage 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.

Table continues…

Name	Description
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 FP Traps webpage 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 FP Traps webpages before starting Master Agent. Use the Agent Status webpage to start or stop Master Agent.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **SNMP** > **FP Traps**.

   The system displays the FP Traps webpage that displays the existing SNMP traps and the status of Master Agent.

2. Click **Add/Change**.
3. Enter the appropriate information in the fields.
4. Click **Submit**.

Related links

Configure SNMP trap destinations field descriptions on page 304

Configure SNMP trap destinations field descriptions

Name	Description
SNMP Version	The three final fields on this page are blank if you use SNMP Version 1 or Version 2c.
IP address	The IP address of the NMS destination or SAL Gateway.
Notification	Displays traps or inform requests.
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: • 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 • AES128
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)** > **SNMP** > **FP Traps**.
2. Check the status of Master Agent.

   Master Agent status must be in **Down** state before you make changes in the FP Traps webpage. 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)** > **SNMP** > **Agent Status**.
   b. On the Agent Status webpage, click **Stop Master Agent**.
   c. After **Master Agent status** is **Down**, on the **Administration** menu, click **Server (Maintenance)** > **SNMP** > **FP Traps**.
4. In the **Current Settings** area on the FP Traps webpage, 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)** > **SNMP** > **Agent Status**.
2. Click **Start Master Agent**.

Deleting an administered SNMP trap

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **SNMP** > **FP Traps**.
2. Check the status of Master Agent.

   Master Agent status must be in **Down** state before you make changes to the FP Traps webpage. 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)** > **SNMP** > **Agent Status**.
   b. On the Agent Status webpage, click **Stop Master Agent**.
   c. After **Master Agent status** is **Down**, on the **Administration** menu, click **Server (Maintenance)** > **SNMP** > **FP Traps**.
4. In the **Current Settings** area on the FP Traps webpage, select the check box associated with the trap that you want to delete.
5. Click **Delete**.

   The FP Traps webpage 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)** > **SNMP** > **Agent Status**.
2. Click **Start Master Agent**.

SNMP filter administration

Use the Filters webpage to do 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 the alarms that are sent as traps to the trap receivers that are administered using the SNMP Traps webpage.

Important:

The system does not display the filters created by Avaya Fault and Performance Manager (FPM) on the Filters webpage. If you are using FPM, create the filters using the FPM application. The FPM application provides additional capabilities that are unavailable using the Filters webpage.

Related links

Configure SNMP trap destinations field descriptions on page 304

Adding an SNMP filter

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **SNMP** > **FP Filters**.
2. Click **Add**.
3. Enter the appropriate information in the fields.
4. Click **Add**.

   The Filters webpage displays the new filter.

Related links

Add FP Filter field descriptions on page 307

Changing an SNMP filter

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **SNMP** > **FP 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 FP Filters webpage displays the changes made to the filter.

Deleting one or all SNMP filters

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **SNMP** > **FP 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 FP Filters webpage.
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 FP Filters webpage.

Add FP 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.

Table continues…

Name	Description
Equip-Type	Select an **Equip-Type** from the following list: • **Cabinet** • **Media Gateway** • **Port** • **Board Number** • **Extension** • **Trunk Group/Member** • **None**

Administering an SNMP Agent

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **SNMP** > **Agent Status**.
2. Check the status of Master Agent.

   Master Agent status must be in **Down** state before you make changes to the Agent Status webpage. 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)** > **SNMP** > **Agent Status**.
   b. On the Agent Status webpage, click **Stop Master Agent**.
   c. After **Master Agent status** is **Down**, on the **Administration** menu, click **Server (Maintenance)** > **SNMP** > **Agent Status**.
4. Enter the appropriate information in the fields.
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)** > **SNMP** > **Agent Status**.
   b. Click **Start Master Agent**.

Important:

You can use the Agent Status webpage 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.

Related links

SNMP Agent Statuss field descriptions on page 309

Agent Status field descriptions

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.

Table continues…

Name	Description
SNMP Version 2c: 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 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

About this task

The Agent Status webpage 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)** > **SNMP** > **Agent Status**.

   The Agent Status webpage 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

About this task

Use the FP Trap Test webpage 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)** > **SNMP** > **FP Trap 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. The port usage logs are only available for a single server or an application server.
- 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

Select Log Types (multiple log output will be merged)

Name	Description
Logmanager debug trace	To view information about Messaging and High Availability Platform software, such as restarts, initializations, shutdowns, process errors, system alarms, and the communication with the external gateways and the port networks. The log rolls over when the log reaches the size limit.
Linux syslog	To view Messaging start information, kernel messages, platform alarms, Messaging alarms, Messaging IP events (if enabled), cron jobs, and general Linux information messages. Linux and platform software use this log.
Linux kernel log	To view information about kernel messages.
Linux access security log	To view 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	To view information about Linux log in and log out procedures and the system restart process.
Linux file transfer log	To view information about files copied to or retrieved from the system. The log indicates the time, user, and files that are copied to or retrieved from the system.
Watchdog logs	To view information about application starts, restarts, failures, shutdowns, heart beating, and Linux restart. The log also contains information about processes that use excessive CPU cycles. Only the watchdog process updates this log. The watchdog logs do not contain specific information about Messaging. If you need information about processes and call processing, see the logmanager debug trace log.
Platform command history log	To view information about webpage access, webpage activity, and bash commands. Use the *bashhis* view to display the bash commands.
HTTP/web server error log	To view the errors and events generated by the web platform server and includes web server restart, abnormal CGI script file terminations, and certificate mismatches.
HTTP/web SSL request log	To view the requests made to the web servers SSL module. Indicates the pages requested or placed in the secure mode.
HTTP/web access log	To view the HTTP/web access log.

Table continues…

Name	Description
Communication Manager Restart log	To view the log that contains the last 16 restarts of the server, including the level of the restarts, the reason for restart requests, and any escalations.

or Select a View (selecting multiple Views may give odd results)

Name	Description
IP events (interfaces up/down; telephone/ endpoint registration/unregistration)	To view IP events. 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	To view the log that 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 scheduled task log (CRON)	To view the log that displays information from the Linux scheduling daemon.
Communication Manager's hardware error and alarm events	To view events that go into the Messaging hardware error and alarm logs.
Communication Manager's software events	To view events that go into the Messaging software error log and needs special deciphering by an external tool.

Table continues…

Name	Description
System update/patch event	To view update tool events that include the following information: • The type of update tool script used for a particular update file. • Additional information about certain update tool scripts indicating if a process stopped and restarted. • The status of the update tool indicating if the update tool ran successfully.
Communication Manager's denial events	To view information about unexpected events that are caused by mismatched translation, mismatched provisioning, network problems, invalid operation, and resource exhaustion. The view displays the denial events on the system.

Select Event Range

Name	Description
Today	To view the events that occurred today.
Yesterday	To view the events that occurred yesterday.
View entries for this date and time	To view the entries for the specified date and time.
Match Pattern	To limit your search by entering the keyword. For example, a name or a message type.

Display Format

Name	Description
Number of Lines	To view the number of lines you have entered.
Newest First	To view the most recent text line.
Remove Header	To view the text without header.

System log results

When you click **View Log** on the System Logs webpage, 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.

   The system displays the administration history log.

Administration History Log field descriptions

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

Table continues…

Name	Description
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

Name	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 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

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.
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

Name	Description
Date	The date the system generated the logs.

Table continues…

Name	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 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.

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

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**

Table continues…

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.
Alarm Code	The alarm code that identifies the reason for the alarm against the specific resource.

Alarm Log Results field descriptions

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 Events, Alarms, and Errors Reference*.
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 links

Alarm Log field descriptions on page 324

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

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

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.

Table continues…

Name	Description
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.
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	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 types of messages: • Errors, indicated by ERR • Resolutions, indicated by RES • Events, indicated by EVN
Report Resource Type	The logical resource type that 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

Name	Description
Administration/Event Log	Records occurrences that are informational or require administrator intervention.

Table continues…

Name	Description
IMAP4 Log	Records errors and events occurred in the communication between the 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 reason. Additional information includes the Far-end IP address and port, mailbox-number, and time.
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.
SMTP (Postfix) Logs	Records data about the routing and delivery of emails, including all errors.

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

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.

Table continues…

Name	Description
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.

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

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.
MWI	The option that indicates if MWI is enabled or disabled for the user.
Date	The log date.
Time	The log time.

Table continues…

Name	Description
Activity	The activity identifier, which is a string that indicates the type of activity for each log entry. For example: • **received**: Message received in this mailbox. • **db-conn**: Database access started for this mailbox. • **db-disconn**: Database access ended for this mailbox. • **inbox-sel**: The IMAP4 “select” command or POP3 login. • **inbox-dsel**: The POP3 logout or any IMAP4 request that “closes” INBOX , including the IMAP4 “unselect” and “close” command. • **status**: Message status changed. • **inbox-stat**: The IMAP4 “ status” command. • **scheduled**: Message sent from this mailbox. • **mwi-off**: MWI turned off. • **mwi-on**: MWI turned on. • **chg pwd**: PIN changed. • **forwarded**: Message auto-forwarded. Appears for foreign stores to show when a message is resent to the foreign store. • **blocked-mb**: Message delivery blocked due to the configuration of the **Block Message Delivery** feature.
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. For example, if you want to trace a problem with the 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.

   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

Filter log messages with these options.

Name	Description
Date Interval	Changes the number of days included in the log filter. The options are: • **Specific**: Filters all the events by the period defined in the Start date (MM/DD) and End date (MM/DD) parameters. • **Last Day**: Filters all the events from the last day. This is the default value. • **Last 2 Days**: Filters all the events from the last 2 days. • **Last 3 Days**: Filters all the events from the last 3 days. • **Last 7 Days**: Filters all the events from the last 7 days. • **Last 14 Days**: Filters all the events from the last 14 days. • **Last 30 Days**: Filters all the events from the last 30 days. • **All**: Disables the filter of the log by the number of days or a specific period.
Category	The system component using which you can filter the system log. The options are: • **All** • **Voice Browser** • **Infobridge** • **Cache** • **Configuration** • **Hardware** • **Telephony Integration Summary** • **Telephony Integration Details** • **AxC**

Table continues…

Name	Description
Severity	The severity level to filter the system log. The options are: • **All** • **Err** • **Warning** • **Notice** • **Info** • **Debug**
Channel (optional)	The affected channel to filter the system log. The values are from *-1* to *99*.
Session ID (optional)	The session ID to filter the system log.
Tag (optional)	This parameter 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 Channel , Session ID, and Tag is only relevant for certain log events that the support personnel 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

About this task

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.

Viewing the port usage report

Before you begin

Enable macros in Microsoft Office.

Procedure

1. Download the port usage log to your system.
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 box 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.

   Do not compare the port usage report to the voice channel monitor display because both measure data differently.

   The port usage report displays the activity of the actual SIP channels while the voice channel monitor displays the activity of the virtual SIP channels.

Related links

Accessing audit and ports usage files on page 338
Port Usage Report descriptions on page 340

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.

Table continues…

Worksheet	Description
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. • 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.

Table continues…

Worksheet	Description
	- Port #1 Outbound Activations: The number of times the system activated the port for outbound use. - 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.

Table continues…

Worksheet	Description
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. • 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

About this task

Using the Diagnostics Results (Application) webpage, you can access 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) webpage displays a list of diagnostic logs.

2. To download all diagnostic logs as a zip file, click **Download**.
3. To download a specific diagnostic log, click the particular log.

Related links

Running application server diagnostics on page 422

Sending logs to an external syslog server

Use the Server Log Files web page to select the logs that the system sends to an external syslog server. The Server Log Files 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** > **Server Log Files**.
2. Enter the appropriate information in the fields.
3. Click **Submit**.

   The system saves the changes.

Server Log Files field descriptions

Control File Synchronization of Syslog Configuration

Name	Description
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	Disables logging to an external syslog server.
Enable logging to the following syslog server	Enables logging to the syslog server that you specify in the Specify the Syslog Server to Receive Events area.

Specify the Syslog Server to Receive Events

Name	Description
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, such as `www.asite.com`, or a literal address. For an IPv6 network, the literal address can be a global unicast address, such as `2002:8709:b5fe:: 75`, or a link local address, such as `fe80::2ca:feff:fe03:5053%eth0`.

Select Which Logs Are to be Sent to the Above Server

Name	Description
boot, cron, *.emerg logs	Select this check box to send the boot, cron, and *.emerg logs to the external server.

Table continues…

Name	Description
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.

Command history

Name	Description
Number of months to store command history	Specifies the number of months for which the command history log is maintained on the system. The range is 3 to 24 months.
Enable compression	Specifies whether the system compresses command history log files to save disk space. Select the check box to enable compression.

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 • Info Mailboxes • Remote Users • Uninitialized Mailboxes • Login Failures • Locked Out Users • Sites • Dormant Mailboxes • Full Mailboxes • Web Access

Table continues…

Report	Description
System Evaluation Report	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 for 30 days. • A new mailbox that has not received any messages for 30 days.
IMAP Traffic(Storage)	Provides a daily or hourly summary of port usage on the Messaging system. Use the report to determine if the Messaging system is performing efficiently by checking information about *outcalling* ports, user traffic, and feature traffic.
SMTP Log Summary (Storage)	Provides the total traffic for all servers with the specified connection type. Also displays the total number of updates.
Measurements (Storage)	Displays daily measurements of traffic by: • Community • Feature • Load • Network load • User

Viewing the local users report

Procedure

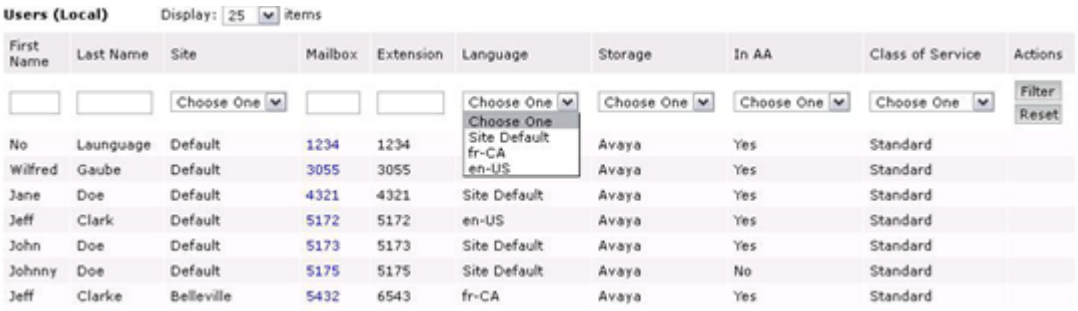
On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.

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 24.
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

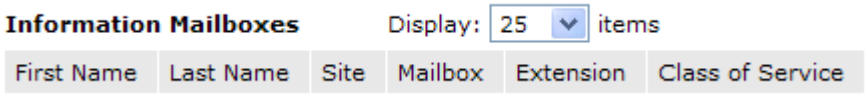
On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Info Mailboxes**.

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

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
Common Name	The common 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.
Extension	The telephone extension of the user.
Numeric Address	The numeric address of the user.
Email Address	The email address of the mailbox of the user.
Community	The community of the user.

Viewing the uninitialized mailboxes report

Procedure

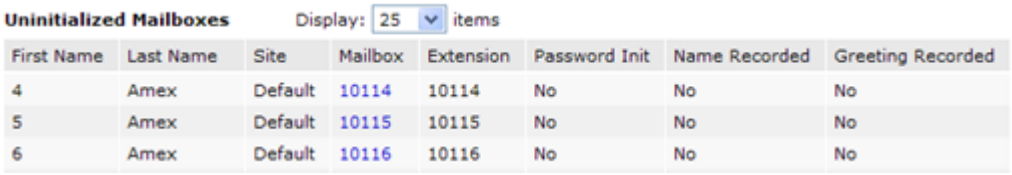
On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Uninitialized Mailboxes**.

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.
Extension	The user extension.

Table continues…

Name	Description
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* • *No*: You must change your password at first logon.
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* • *No*: You must record your name at first logon.
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* • *No*: You must record a personal greeting at first logon.

Viewing the login failures report

Procedure

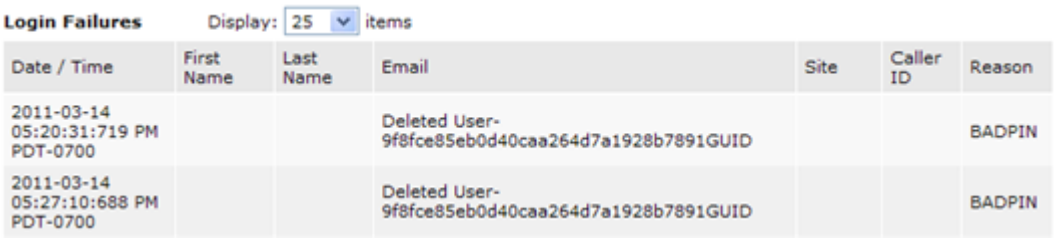
On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Login Failures**.

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.

Viewing the Sites report

Procedure

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

Tip:

Select the options in the drop-down list of the following fields to filter the report result:

- **Extension Style**
- **Site Default Language**
- **Auto Attendant Enabled**
- **Auto Attendant Speech Recognition Enabled**
- **Telephony Profile Name**

- **Customized Greeting Enabled**

Sites report field descriptions

Name	Description
Display	The option to control the number of sites displayed on each page of the report. The options are: • 25 • 50 • 100 • All
Description	The name of the site. You can click the link to identify the site and modify the properties for that site.
Active Appliances	The application server of the site.
Extension Style	The extension style for the telephony integration.
Country Code	The digits that identify each country in the world. The country code is one, two or three digits.
Site Prefix	The digits that precede the extension in a phone number.
Internal Messaging Access Number	The number and prefix that Messaging expects to receive from the telephony server.
Short Mailbox Length	The mailbox number length for the users of the site.
Short Extension Length	The extension length for the users of the site.
Number Of Users	The total number of users in the site.
Site Default Language	The default language administered for the site.
Auto Attendant Enabled	The option to filter the Sites report for the list of sites with Auto Attendant enabled or disabled.
Auto Attendant Speech Recognition Enabled	The option to filter the Sites report for the list of sites with Auto Attendant Speech Recognition enabled or disabled.
P-Asserted Identity Name	The name administered in the identity information of the P-AI header.
P-Asserted Identity Number	The number administered in the identity information of the P-AI header.
Telephony Profile Name	The profile name of the far-end SIP domain.

Table continues…

Name	Description
Customized Greeting Enabled	The option to filter the Sites report for the list of sites with Customized Greeting feature enabled or disabled.
Action	The option to: • Generate the filtered Sites report • Reset the filters • Add user

Viewing the Dormant Mailboxes report

About this task

Generate a list of mailboxes that have not been logged in to or received messages for the specified number of days. The specified period is the dormant period.

Procedure

1. On the **Administration** menu, click **Report (Storage)** > **Dormant Mailboxes**.
2. To generate the Dormant Mailboxes report, click **Run**.

   You can specify the number of days for the dormant period in the **Dormant Period (Days)** field. The value range is from 1 to 3650 days. For example, if you specify the dormant period as 30, Messaging generates the report with a list of mailboxes that have been dormant for 30 days.

   In the **Days since Mailbox Database Created/Rebuilt** field, you can specify a value.

   This value indicates how many days have elapsed since the mailbox database was created or rebuilt.

   Messaging displays a list of mailboxes that have been dormant for the specified period.

   - If you recently rebuilt the mailbox database for a system restoration, system upgrade, or a similar activity Messaging displays a message. This message indicates that insufficient time has passed since the last database rebuild to determine dormant mailboxes. Messaging also displays a message when there are no dormant mailboxes.
   - In the **Days Since Last Access** column, the report categorizes the uninitialized mailboxes, which have not been logged in to or received messages, as **Not Accessed**. When you download the list, the report categorizes these mailboxes as **uninitialized**.

Dormant Mailboxes report field descriptions

Name	Description
Subscriber Name	The name of the subscriber whose mailbox is dormant for the number of days specified in **Dormant Period (Days)**.
Mailbox Number	The number of the mailbox that is dormant for the number of days specified in **Dormant Period (Days)**.
Extension	The extension number of the mailbox that is dormant for the number of days specified in **Dormant Period (Days)**.
Days Since Last Access	The number of days since the subscriber last logged in to the dormant mailbox.

Viewing the Full Mailboxes report

About this task

Generate a list of mailboxes whose storage capacity usage has exceeded the specified threshold percentage.

Procedure

1. On the **Administration** menu, click **Messaging** > **Report (Storage)** > **Full Mailboxes**.
2. To generate the Full Mailboxes report, click **Run**.

   Specify the percentage of the storage capacity that Messaging uses to generate the report in the Threshold Percentage field. The value range is from *50* to *100*%. For example, if you specify the threshold percentage as *75*, Messaging generates the report with a list of mailboxes that have reached 75% of the storage capacity.

   Messaging displays a list of mailboxes that have exceeded the specified storage capacity threshold percentage. The report does not include mailboxes stored on an external storage.

Full Mailboxes report field descriptions

Name	Description
Subscriber Name	The ASCII name of the subscriber.

Table continues…

Name	Description
Mailbox Number	The mailbox number of the subscriber.
Percent Full	The percentage of the allocated total mailbox storage capacity used. The capacity usage of mailboxes might display a usage above 100% because mailboxes can exceed their allocated storage capacity under certain conditions. The User Preferences page displays the percentage of unutilized storage space.
Max. Space (KB)	The total amount of storage capacity allocated to the mailbox in KB.
Site ID	The ID of the site where the mailbox is located.

Viewing the Web Access report

About this task

The Web Access report displays the following data for the number of days that you specify:

- The number of times that users logged in and logged out each day.
- The number of time that users logged in and logged out each hour of a specific date.

The report provides data for a maximum of 30 days.

Procedure

1. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Web Access**.
2. In the **Select date interval** field, select the number of days.
3. Click **Show Reports**.

   Messaging displays the number of times that user logged in and logged out each day for the number of days that you specify.
4. To view the number of time that users logged in and logged out in one hour for a specific day:
   a. In the **Count of logins per hour** section, select the date.

      Messaging displays the **Count of logins per hour** section only after you run the report for a specific number of days.
   b. Click **Show report**.

   Messaging displays the number of times that users logged in and logged out in one hour for the number of days that you specify.

Web Access Reports field description

Name	Description
Select date interval	The number of days to include in the report. You can view the information for a maximum 30 days.
Web Access Login Metrics	
Count of logins per day	The IP address of the application server and the number of times users logged in to Messaging Web Access for each day in the specified period. Messaging displays this section after you click **Show Reports**.
Count of logins per hour	The IP address of the application server and the number of times users logged in to Messaging Web Access for each hour of the day that you select in **Select date**. Messaging displays this section after you click **Show Reports**.
Select date	The day for which Messaging generates the hourly report.

Running the system evaluation report

About this task

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**.

   The system displays the report.

2. To refresh the report, click **Re-run System Report**.

   The System Evaluation Report webpage 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 Traffic (Storage)**.

   The system displays a security warning if the system cannot verify the certificate of the Web site. Click **Yes** to continue.

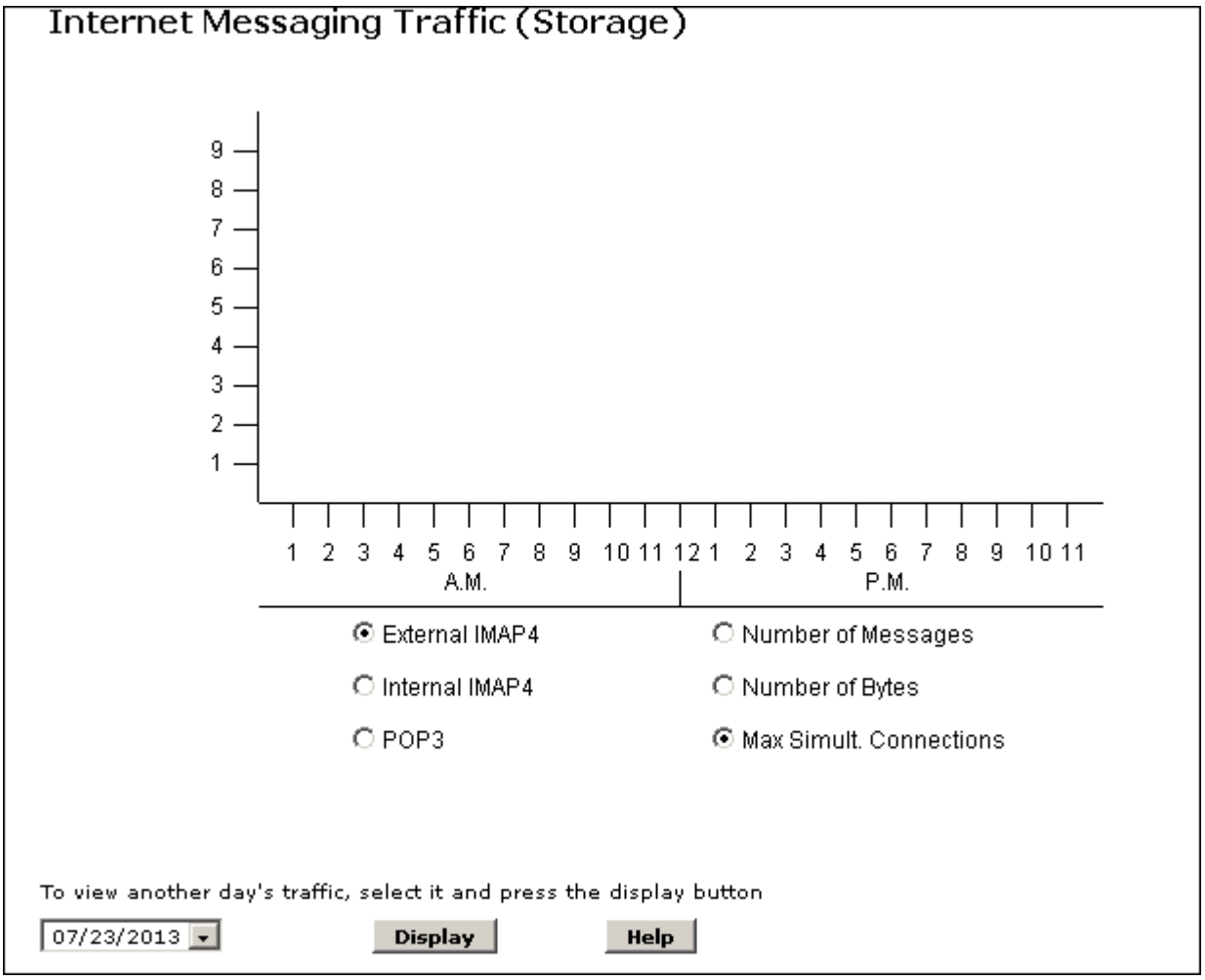
   The Internet Messaging Traffic (Storage) webpage displays a graph of the traffic for the selected days.

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 (Storage) field descriptions

Name	Description
X-axis	X-axis displays the time of day in hours.

Table continues…

Name	Description
Y-axis	The Y-axis options are: • **External IMAP4** - **Number of Messages** - **Number of Bytes** - **Max Simult. Connections**: The maximum number of simultaneous IMAP sessions for each hour of the selected day. • **Internal IMAP4** - **Number of Messages** - **Number of Bytes** - **Max Simult. Connections**: The maximum number of simultaneous IMAP sessions for each hour of the selected day. • **POP3** - **Number of Messages** - **Number of Bytes** - **Total Sessions**: The total POP3 sessions for each hour of the selected day. The values of Y-axis change based on the option selected in the right column.

Viewing the SMTP log summary

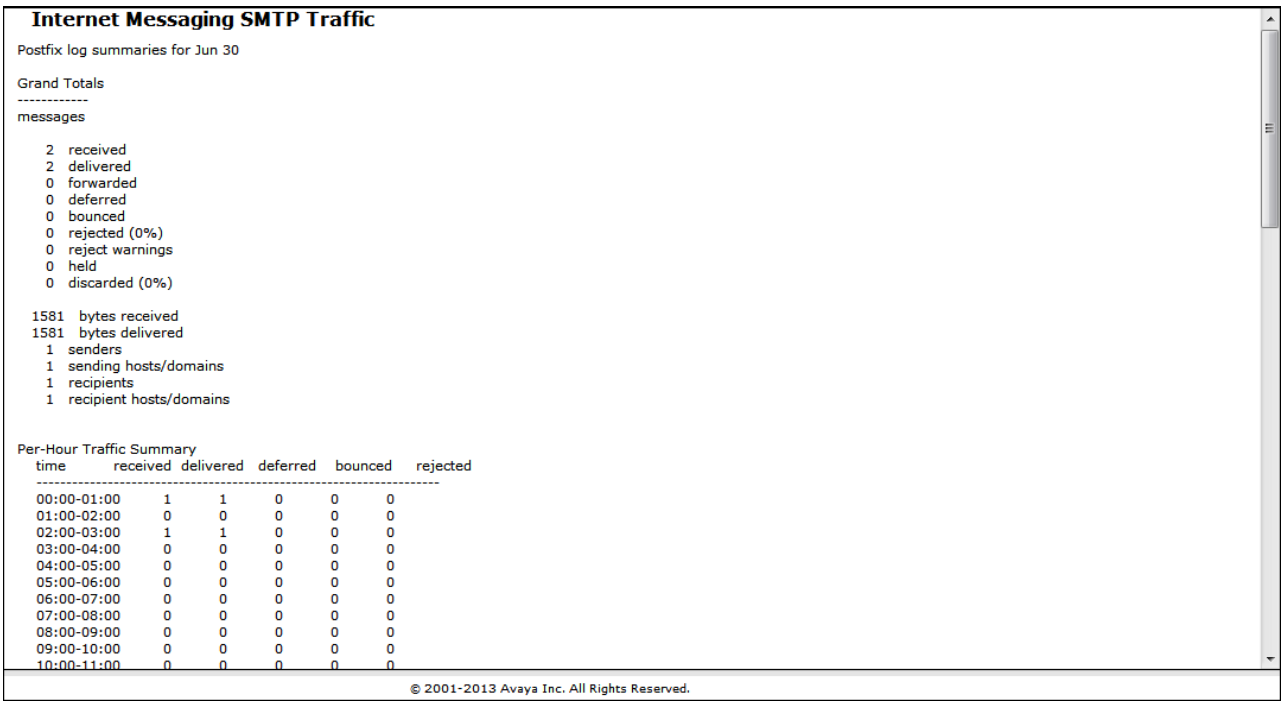
Procedure

On the **Administration** menu, click **Messaging** > **Server Reports** > **SMTP Log Summary (Storage)**.

The SMTP Log Summary (Storage) webpage displays a summary of the SMTP traffic.

Example

The following image is an example of the SMTP Log Summary (Storage) webpage.



Internet Messaging SMTP Traffic

Postfix log summaries for Jun 30

Grand Totals
---
messages

2 received
2 delivered
0 forwarded
0 deferred
0 bounced
0 rejected (0%)
0 reject warnings
0 held
0 discarded (0%)

1581 bytes received
1581 bytes delivered
1 senders
1 sending hosts/domains
1 recipients
1 recipient hosts/domains

Per-Hour Traffic Summary

time	received	delivered	deferred	bounced	rejected
00:00-01:00	1	1	0	0	0
01:00-02:00	0	0	0	0	0
02:00-03:00	1	1	0	0	0
03:00-04:00	0	0	0	0	0
04:00-05:00	0	0	0	0	0
05:00-06:00	0	0	0	0	0
06:00-07:00	0	0	0	0	0
07:00-08:00	0	0	0	0	0
08:00-09:00	0	0	0	0	0
09:00-10:00	0	0	0	0	0
10:00-11:00	0	0	0	0	0

Running the traffic measurement report

About this task

Use the Messaging Measurements web page to request traffic measurements from the Messaging system.

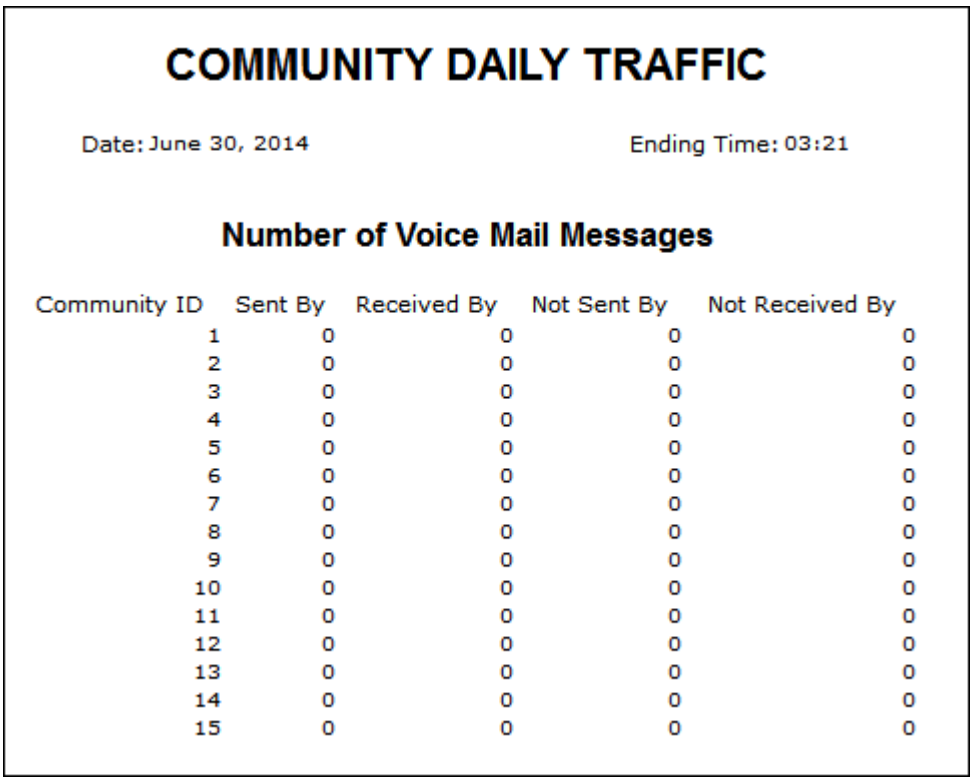
Procedure

1. On the **Administration** menu, click **Messaging** > **Server Reports** > **Measurements (Storage)**.
2. From **Type**, select the required traffic type.
3. Click **Get Report**.

   The system displays the report for the traffic type that you select.

Example

The following image shows the columns in the community traffic measurements report.



COMMUNITY DAILY TRAFFIC

Date: June 30, 2014 Ending Time: 03:21

Number of Voice Mail Messages

Community ID	Sent By	Received By	Not Sent By	Not Received By
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0

Related links

Community daily and hourly traffic report on page 367
Feature daily and hourly traffic report on page 368
Load daily and hourly traffic report on page 371
Subscriber daily and monthly traffic report on page 374

Messaging Measurements field descriptions

Name	Description
Type	The types of traffic. The options are: • **Community**: Displays daily or hourly measurements of the messages sent and received by the community users. • **Feature**: Displays information on a feature-by-feature basis. The features are: - Remote subscriber - Voice mail - Call answer • **Load**: Displays information for both user thresholds and voice ports. Traffic load refers to the number of calls that each active port handles. • **Network-Load**: Displays information about the network channel traffic. • **Remote Messages**: Displays information about the message traffic between the local system and a remote system. • **Subscriber**: Displays information about a specific subscriber. This report tracks the mail use pattern of a particular subscriber. • **Traffic Snapshot**: Displays information about messaging traffic snapshots. For more information on the reports for different traffic types, see Running the traffic measurement report.
Cycle	The frequency at which various traffic types collect traffic data. The available frequency options depend on the selected traffic type as follows: • Community, Feature, Load, or Network-Load: - **Hourly**: Up to 192 hours (8 days) - **Daily**: Up to 32 days • Subscriber, Remote Messages, or Traffic Snapshot: - **Daily**: Up to 8 days - **Monthly**: Up to 13 months

Table continues…

Name	Description
Start Date	The scheduled date to start traffic data collection.
Mailbox Number	The mailbox number of the subscriber. The system displays the mailbox number field only when you select the **Subscriber** type.

Button description

Name	Description
Get Report	Displays the measurement report for the traffic types.

The system displays the following buttons when you click **Get Report**.

Name	Description
Previous day	Displays the measurement traffic report for the date previous to the current date.
Clear Report	Clears the selection.
Next day	Displays the measurement traffic report for the date after the current date.

Community daily and hourly traffic report

Use the community traffic report to analyze the number of messages sent and received by each community for the specified period.

You can analyze the community traffic one day at a time for up to 32 days or one hour at a time for up to 192 hours (8 days). By default, the system displays a report on a daily basis. If you want to review the report on a hourly basis, in **Cycles**, select **Hourly**.

Name	Description
Community ID	The community number that you administer for users or class of services.
Sent by	The total number of messages sent by all members of each community during the reporting period.
Not Sent by	The total number of messages that all members of each community attempted to send and failed due to sending restrictions.
Received by	The total number of messages received by all members of each community during the reporting period.
Not Received by	The total number of messages that the addressed members of each community did not receive due to sending restrictions.

Feature daily and hourly traffic report

Use the feature traffic report to analyze the traffic information by feature for the specified days or hours. The features are:

- Remote subscriber
- Voice mail
- Call answer

You can analyze the feature traffic one day at a time for up to 32 days or one hour at a time for up to 192 hours (8 hours). By default, the system displays a report on a daily basis. If you want to review the report on a hourly basis, in **Cycles**, select **Hourly**.

REMOTE SUBSCRIBERS

Name	Description
Administered	The total number of remote subscribers on the messaging system at the end of the time period being reported.
Non Administered	The total number of remote non-administered subscribers on the messaging system at the end of the time period being reported.

VOICE MAIL

Name	Description
Administered	The total number of remote subscribers on the messaging system at the end of the time period being reported.
Non Administered	The total number of remote non-administered subscribers on the messaging system at the end of the time period being reported.
Total Messages, Sent	The total number of messages that are sent on the local messaging system during the reporting period. The messages include: • Header-only messages • Messages to remote subscribers • Unaddressed messages • Undeliverable messages • Remote incoming messages The sum of broadcast, priority, and private messages might not equal this total because some messages might be counted twice in the subtotals.

Table continues…

Name	Description
Total Messages, Current	The total number of messages on the local messaging system.
Voice Components, Sent	The total number of voice components that are sent on the local messaging system during the reporting period. The messages include: • Messages to remote subscribers • Unaddressed messages • Undeliverable messages • Remote incoming messages
Voice Components, Current	The total number of voice components on the local messaging system.
Fax Components, Sent	The total number of fax components that are sent on the local messaging system during the reporting period. The messages include: • Messages to remote subscribers • Unaddressed messages • Undeliverable messages • Remote incoming messages
Fax Components, Current	The total number of fax components on the local messaging system.
Binary Attachments, Sent	The total number of binary attachments for voice mail messages that are sent on the local messaging system during the reporting period. The messages include: • Messages to remote subscribers • Unaddressed messages • Undeliverable messages • Remote incoming messages
Binary Attachments, Current	The total number of binary attachments for voice mail messages on the local messaging system.
Text Components, Sent	The total number of text components that are sent on the local messaging system during the reporting period. The messages include: • Messages to remote subscribers • Unaddressed messages • Undeliverable messages • Remote incoming messages

Table continues…

Name	Description
Text Components, Current	The total number of text components on the local messaging system.
Broadcast Messages, Sent	The number of broadcast messages that are sent on the local messaging system during the reporting period. The messages include: • Messages to remote subscribers • Unaddressed messages • Undeliverable messages • Remote incoming messages
Broadcast Messages, Current	The number of broadcast messages on the local messaging system.
Log-in Announcements, Sent	The number of messages that are sent on the local messaging system during the reporting period and that are login announcements.
Log-in Announcements, Current	The number of messages on the local messaging system that are marked as active announcements.
Urgent Messages, Sent	The total number of priority voice messages that are sent on the local messaging system during the reporting period. These voice messages are marked for urgent delivery. The messages include: • Messages to remote subscribers • Unaddressed messages • Undeliverable messages • Remote incoming messages
Urgent Messages, Current	The number of messages on the local messaging system that are marked as urgent messages.
Private Messages, Sent	The total number of private voice messages that are sent on the local messaging system during the reporting period. These voice messages are marked for private delivery. The messages include: • Messages to remote subscribers • Unaddressed messages • Undeliverable messages • Remote incoming messages
Private Messages, Current	The number of messages on the local messaging system that are marked for private delivery.
Average Storage Time	The average duration in minutes for the hour being reported that messages remained in the system before being deleted.

CALL ANSWER

Name	Description
Total Messages, Received	The total number of call answer messages recorded by the local machine during the reporting period.
Total Messages, Current	The total number of call answer messages stored on the local messaging system.
Voice Components, Received	The total number of call answer voice components recorded by the local machine during the reporting period.
Voice Components, Current	The total number of call answer voice components stored on the local messaging system.
Fax Components, Received	The total number of call answer fax components recorded by the local machine during the reporting period.
Fax Components, Current	The total number of call answer fax components stored on the local messaging system.
Average Storage Time	The average duration in minutes during the day being reported that call answer messages remained in the system before being deleted.

Load daily and hourly traffic report

Use the load traffic report to analyze the number of subscriber warnings issued for crossing prethreshold limits and system storage information in a specified period.

You can analyze the traffic one day at a time for up to 32 days or one hour at a time for up to 192 hours (8 days). By default, the system displays a report on a daily basis. If you want to review the report on a hourly basis, in **Cycles**, select **Hourly**.

TOTAL SUBSCRIBER THRESHOLD EXCEPTIONS

Name	Description
Lists	The number of warnings issued to users who exceed the maximum allowed number of mailing lists during the period being reported.
List space	The number of warnings issued to users who exceed the maximum allowed number of list entries during the period being reported.
Message Space, Lower	The number of warnings issued to users who reach the lower space threshold during the period being reported.

Table continues…

Name	Description
Message Space, Upper	The number of warnings issued to users who reach the upper space threshold during the period being reported.
Subscribers Over Threshold	The number of subscribers who exceeded one or more message space threshold during the period being reported.
Deliveries Rescheduled	The number of message deliveries that could not be completed and were rescheduled or canceled.

SYSTEM STORAGE

Name	Description
Total Storage Free	The minimum free space in megabytes and hours that is available in all voice file systems during the period being reported.
Total Storage Used	The maximum number of megabytes and hours used in all voice file systems during the reporting period.
Message Storage Used	The maximum number of megabytes and hours used for all the messages during the period being reported.
Voiced Named Storage Used	The maximum number of megabytes and hours used for all the names during the period being reported.
Directory Storage Used	The maximum number of megabytes and hours used for the directory during the period being reported.

Network-Load daily and hourly traffic report

Use the Network-Load traffic report to analyze the network channel traffic one day at a time for up to 32 days or one hour at a time for up to 192 hours (8 days).

By default, the system displays a report on a daily basis. If you want to review the report on a hourly basis, in **Cycles**, select **Hourly**.

Name	Description
Date	The starting date for which traffic data was collected for the report. If you enter a date prior to the current date, each day's record is presented as an additional page (screen). Click **Next Hour** and **Previous Hour** to scroll through each hourly report record.
Hour	The starting hour for which traffic data was collected for the report. It is the hour that you entered in the **Hour** or the current hour if you did not specify an hour.
Ending Time	The time at which data collecting ended.
Remote Deliveries Rescheduled	The number of messages that were rescheduled because of transmission difficulties or space limitations on the remote node during the recording period.
Total Remote Undeliverable Messages	The total number of messages that were rejected for delivery to a remote machine because, for example, the remote subscriber was not defined to the local machine.
USAGE (SECONDS)	
Incoming **Outgoing** **Total**	The number of seconds that each network channel was active with incoming and outgoing calls during the recording period. The total seconds of activity are also provided.
PEG COUNT (NUMBER OF SESSIONS)	
Incoming **Outgoing** **Total**	The number of incoming and outgoing calls on each network channel during the recording period. The total number of calls is also provided.

Remote messages traffic report

Use the remote message traffic report to analyze information about message traffic between the local system and a specified remote system.

You can analyze the remote messages traffic one day at a time for up to 8 days or one month at a time for up to 13 months. By default, the system displays a report on a daily basis. If you want to review the report on a monthly basis, in **Cycles**, select **Monthly**.

From the **Machine** drop-down list, you can select the required remote system.

Name	Description
Machine Name	The name of the machine.
Machine Type	The type of machine for the remote machine specified in the **Machine Name** field.
Local Organization	Prime and Non-Prime Headers that indicate that message transmission was originated with the local machine during a period specified as prime or non-prime time.
Remote Organization	Prime and Non-Prime Headers that indicate that message transmission was originated with the remote machine during a period specified as prime or non-prime time.
Transfer Sessions	The number of message transfer sessions that occurred during the collection period.
Usage (seconds)	The total number of seconds for all message transfer session that occurred during the collection period.
Average Usage	The average length in seconds of a message transfer session.
Messages Sent	The total number of messages sent from the local system to the remote system and from the remote system and received by the local system during the collection period.
Messages Rejected	The total number of messages rejected by the local and remote systems during the collection period.
Administrative Updates	The total number of administration updates, such as name, voice, extension, community changes, add and delete local subscribers, sent from the local system to the remote system and sent from the remote system and received by the local system.
Session Failures: Far End No Answer	The number of unsuccessful call attempts from the local system to the remote system.

Subscriber daily and monthly traffic report

Use the subscriber traffic report to analyze the traffic information about a specific subscriber in a specific period.

You can analyze the subscriber traffic one day at a time for up to 8 days or one month at a time for up to 13 month. By default, the system displays a report on a daily basis. If you want to review the report on a monthly basis, in **Cycles**, select **Monthly**.

Name	Description
Name	The name of the user whose traffic information is being reported.
Mailbox number	The mailbox number of the user whose traffic information is reported.
Community ID	The number of the community to which the user belongs.
Mailbox Space Used	The amount of message space in megabytes and minutes used by the subscriber at the end of the period being reported.
Space Allowed	The maximum allowed mailbox size in megabytes and minutes administered for a subscriber during the reporting period.
Maximum Space Used	The maximum amount of message space in megabytes and minutes used during the reporting period.

VOICE MAIL MESSAGES RECEIVED

Name	Description
Local Mail Messages	The number of messages received by the subscriber during the reporting period.
Voice Components	The number of voice components that the subscriber receives from the local machine during the reporting period.
FAX Components	The number of fax components that the subscriber receives from the local machine during the reporting period.
Binary Attachments	The number of binary attachments that the subscriber receives from the local machine during prime and nonprime hours in the reporting period.
Text Components	The number of text components that the subscriber receives from the local machine during the reporting period.
Remote Mail Messages	The number of messages that the subscriber receives from the remote machines during prime and nonprime hours in the reporting period.
Voice Components	The number of voice components that the subscriber receives from the remote machines during prime and nonprime hours in the reporting period.
FAX Components	The number of fax components that the subscriber receives from the remote machines during prime and nonprime hours in the reporting period.

Table continues…

Name	Description
Binary Attachments	The number of binary attachments that the subscriber receives from the remote machines during prime and nonprime hours in the reporting period.
Text Components	The number of text components that the subscriber receives from the remote machines during prime and nonprime hours in the reporting period.
Undeliverable Notifications	The number of times that the system alerts the subscriber about an undeliverable message during the reporting period.

CALL ANSWER MESSAGES RECEIVED

Name	Description
Total Call Answer Messages	The number of new call answer messages in the mailbox of the subscriber during prime and nonprime hours in the reporting period.
Voice Components	The number of new voice components in the mailbox of the subscriber during prime and nonprime hours in the reporting period.
FAX Components	The number of new fax components in the mailbox of the subscriber during prime and nonprime hours in the reporting period.

VOICE MAIL MESSAGES CREATED

Name	Description
Total Voice Mail Messages	The total number of messages created by the subscriber during the reporting period.
Broadcast Messages	The number of broadcast messages created by the subscriber during the reporting period.
Login Announcements	The number of login announcements created by the subscriber during the reporting period.
Urgent Messages	The number of urgent messages created by the subscriber during the reporting period.
Private Messages	The number of private messages created by the subscriber during the reporting period.
Voice Components	The number of voice components created by the subscriber during the reporting period.
FAX Components	The number of fax components created by the subscriber during the reporting period.
Binary Attachments	The number of binary attachments created by the subscriber during the reporting period.

Table continues…

Name	Description
Text Components	The number of text components created by the subscriber during the reporting period.

MESSAGES SENT

Name	Description
Local Messages	The number of messages sent to local subscribers by the subscriber during the reporting period.
Voice Components	The number of voice components sent to local subscribers by the subscriber during the reporting period.
FAX Components	The number of fax components sent to local subscribers by the subscriber during the reporting period.
Binary Attachments	The number of binary attachments sent to local subscribers by the subscriber during the reporting period.
Text Components	The number of text components sent to local subscribers by the subscriber during the reporting period.
Remote Messages	The number of messages sent to remote subscribers by the subscriber during the reporting period.

Traffic snapshot report

Use the traffic snapshot report to analyze messaging traffic snapshots.

You can analyze traffic snapshots one day at a time for up to 8 days or one month at a time for up to 13 months. By default, the system displays a report on a daily basis. If you want to review the report on a monthly basis, in **Cycles**, select **Monthly**.

Name	Description
Connection Type	The connection type.
TRAFFIC TOTAL	The sum of each field for all the machines with the specified connection type
REMOTE MACHINE STATISTICS	Traffic information for each machine with the specified connection type.
MACHINE NAME	The name of the remote machine.
MESSAGES — Sent	The total number of messages sent from the local system to the remote machine.

Table continues…

Name	Description
MESSAGES — Received	The total number of messages received by the local system from the remote machine.
UPDATES — Out	The total number of updates, such as name, mailbox number, or community ID, sent from the local messaging system to the remote machine.
UPDATES — In	The total number of updates, such as name, mailbox number, or community ID, sent from the remote machine and received by the local messaging system.
TRANSFER SESSIONS	The total number of message transfer sessions that occurred during the period specified as prime or non-prime time.
%USAGE	The percentage of usage for all message transfer sessions that occurred during the period specified as prime or non-prime time. The formula to calculate percentage is: %usage = (Total Usage)/(Usage for Period)
MESSAGES — Queued	The total number of messages to be sent from the local system to the remote machine.
STATUS — Queued	The total number of message statuses to be sent from the local system to the remote machine.

Viewing the login reports

About this task

Use the Login Reports webpage 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.

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, type the time period details.
4. In the **Output Format** area, type the appropriate details.
5. To generate the report, click **Continue**.

   The system displays the login report for the selected type.

Login Reports field descriptions

Select an option

Name	Description
List Local Host Logins	To generate a report for all local host logins.
Display Information for Local Host Login	To generate a report for the individual local host login by entering the individual login name.
Display Information for Failed Logins	To generate a report of failed logins.
Display Information for Successful Logins	To generate a report of successful logins.
Display Detailed Information for Successful Logins	To generate a detailed report for the successful logins. The default *all* keyword generates 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

Name	Description
Start Day/Time	To enter the start time for the report in the format mm:dd and HH:MM.
End Day/Time	To enter the end time for the report in the format mm:dd and HH:MM.

Output Format

Name	Description
Enter Maximum Number of Lines to Display	To enter the maximum number of lines to display. The default value is 200.
Display Reports Newest First	To display the newest reports first.

Viewing the outbound fax status

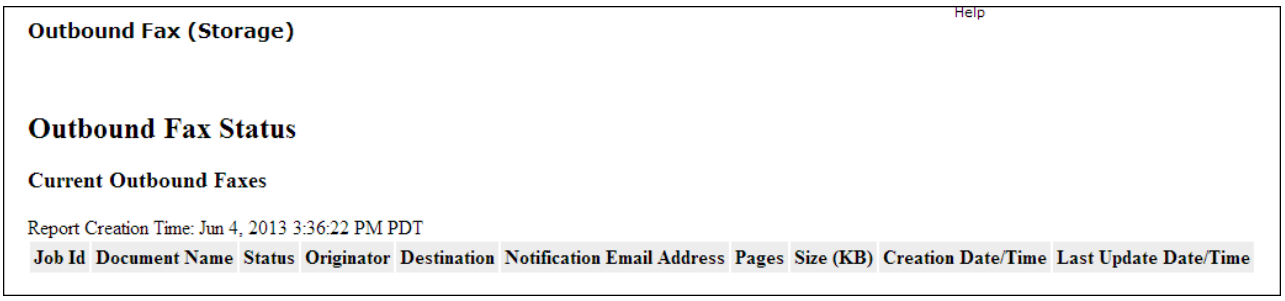
Procedure

On the **Administration** menu, click **Messaging** > **Server Information** > **Outbound Fax (Storage)**.

The Outbound Fax (Storage) page displays the information about all faxes sent by Messaging users. This page automatically refreshes every 15 seconds.

Example

The following image is an example of the Outbound Fax (Storage) report:


Help

Outbound Fax (Storage)

Outbound Fax Status

Current Outbound Faxes

Report Creation Time: Jun 4, 2013 3:36:22 PM PDT

Job Id	Document Name	Status	Originator	Destination	Notification Email Address	Pages	Size (KB)	Creation Date/Time	Last Update Date/Time

Outbound Fax (Storage) field descriptions

Name	Description
Job Id	The fax job identifier.
Document Name	The name of the fax document.
Status	The current status of the fax job.
Originator	The user who sent the fax.
Destination	The destination of the fax.
Notification Email Address	The email address of the user who sent the fax. This email address is used to notify the user about the final status of the fax job.
Pages	The number of pages in the fax job.
Size (KB)	The size of the fax job.
Creation Date/Time	The date and time when the user sent the fax.
Last Update Date/Time	The date and time when the fax job was updated.

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 the **Administration** menu, and then clicking **Server (Maintenance)** > **Alarms** > **Current Alarms**.

Related links

Application server on page 381
Storage server on page 383

Application server

Number	Tasks	Links	Frequency
1	Check the port usage report.	For more information, see: • Accessing audit and ports usage files on page 338 • Viewing the port usage report on page 339	Daily.
2	Check the alarm log. The log displays active alarms and resolved alarms.	For more information, see: • Logs overview on page 312 • Viewing the alarm logs on page 324	Daily.
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 312 • Viewing the system logs on page 313	Daily.

Table continues…

Number	Tasks	Links	Frequency
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 282 • Backing up application files on page 287	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.
6	Verify that the backup completed successfully.	For more information, see Viewing backup logs on page 292.	Daily.

Table continues…

Number	Tasks	Links	Frequency
7	Restore the data.	For more information, see: • Back up and restore overview on page 282 • Performing a restore on page 294	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://support.avaya.com.		Monthly.
9	Reboot the application server.	For more information see, Shutting down the server on page 456.	As necessary or once a year.

Related links

Maintenance checklist on page 381

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 Events, Alarms, and Errors Reference* document.	Daily.
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 320. • User activity logs on page 331. • Configuring a user activity log on page 331. • Running an activity log report on page 332.	Daily.

Table continues…

Number	Tasks	Links	Frequency
3	Check the alarm log. The log displays active alarms and resolved alarms.	For more information, see: • Storage server logs overview on page 320. • Viewing the alarm logs on page 324.	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 320. • Viewing the administration history log on page 321. • Viewing the administrators log on page 322.	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 291. • Viewing backup logs on page 292.	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 206.	As necessary.
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 **Consecutive Invalid Attempts** field on the System Administration webpage 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 207. • Viewing the locked out users report on page 354.	As necessary.
8	Reboot the storage server.	For more information see, Shutting down the server on page 456.	As necessary or once a year.

Table continues…

Number	Tasks	Links	Frequency
9	Check the Linux system clock.	For more information, see Verifying the system clock on page 41.	Monthly and when a daylight-saving time change occurs.
10	Add, delete, or change local users to maintain user profiles that reflect current needs and staffing.	For more information about how to manage local users, see: • Adding users on page 189. • Adding users from Active Directory on page 190. • Changing user properties on page 191. • Deleting users on page 192. • Viewing the local users report on page 348.	As necessary.
11	Administer remote users. A remote update can use one of your networking ports for a long 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 209. • Running a remote update manually on page 211. • Viewing the remote users report on page 350.	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 70. • Configuring the postmaster mailbox number on page 71.	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 352.	Monthly.
14	Check the dormant mailbox report to identify inactive mailboxes.	For more information, see Running the system evaluation report on page 360.	Monthly.

Table continues…

Number	Tasks	Links	Frequency
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 361. • Running the traffic measurement report on page 364.	As necessary.
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 387. • Performing the voice messaging database audit on page 388. • Running Audit on page 389.	As necessary.
17	Back up the data.	For more information, see: • Back up and restore overview on page 282. • Backing up the system on page 284.	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 292.	Daily.

Table continues…

Number	Tasks	Links	Frequency
19	Restore the data.	For more information, see: • Back up and restore overview on page 282. • Performing a restore on page 294.	Do 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 241.	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 320. • Viewing the software management logs on page 326.	As necessary.

Related links

Maintenance checklist on page 381

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. The mailbox audit that is also a part of the nightly audit sends MWI updates for local users on the system.
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.
Start Subscriber Data Audit (Subscribers, Delivery Data)	Audit user data. The subscriber data audit that is also a part of the nightly audit fixes errors and sends correct MWI updates for local users on the system.
Start Nightly Audit (Nightly, Delivery Data)	Perform nightly audit.

Table continues…

Click	To
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.

Performing MWI audit

About this task

Use this procedure to perform audit for MWI from the command line interface.

The two audits are:

- Subscriber translation audit.
- MWI audit.

Procedure

On the **Administration** menu, click **Messaging** > **Utilities** > **Messaging DB Audits (Storage)** > **Start Subscriber Data Audit**.

The subscriber data audit that is also a part of the nightly audit fixes errors and sends correct MWI updates for local users on the system.

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

About this task

The Services Restart (Storage) webpage 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** > **Services Restart (Storage)**.
2. Verify if all processes are in the **UP** state.
3. If any process is not in the **UP** state, click **Restart** to manually start the process.
4. Restart the Messaging application. The system starts all LDAP processes.

Services Restart (Storage) field descriptions

Name	Description
slapd	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. The options are: • **UP**: Indicates that slapd is running. • **DOWN**: Indicates that slapd is not running and you must restart Messaging.
Ldapfe	The process to do the administration from the webpages. The options are: • **UP**: Indicates that Ldapfe is running. • **DOWN**: Indicates that Ldapfe is not running. You can do the administration through the webpages until you restart this process.
Ldapcorp	The process to do the administration from external LDAP clients. The firewall must also be open to do the administration through external clients. The options are: • **UP**: Indicates that Ldapcorp is running. • **DOWN**: Indicates that Ldapcorp is not running. You can do the administration through the external LDAP clients until you restart this process.

Table continues…

Name	Description
faxprinter	The option to restart the faxprinter service. If the server role is storage only or application and storage, a new option is available to restart the faxprinter service. If you restart this service, then the outbound faxes that are in progress or in the repository are stopped. When you click **Restart**, the system displays a pop-up confirmation box to confirm the restart request.

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. 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. The maximum value for this option is upto 100.
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. The maximum value for this option is upto 100.

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

About this task

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.

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 **User List**.

Related links

Loading lists on page 146

Mail Options field descriptions

Name	Description
Mailbox Gateway Machine Name	The TCP/IP host name of the mailbox gateway. Your communication network routes all outbound emails through the gateway that you select from this drop-down list. The system populates the list using the External Hosts web page.
Mailbox Gateway Machine Port	The port that Messaging uses to connect to the mailbox gateway. The default port is 25.

Table continues…

Name	Description
Server Alias	Any legal domain name. Server aliases allow your company clients and employees to use easily recognized email addresses instead of the default ones. The default email address has the `<username>@<hostname>.<domain>` format. A server alias allows to “hide” the host name in the address and use the `<username>@<domain>` address format. For example: • Default address without an alias: `user@machine.company.com` • Address with an alias: `user@company.com` In this example, `machine` is the host name and `company.com` is the domain name.
Warn about undeliverable mail after	The number of days after which the system notifies users that the system did not deliver the user message. The options are: • Days • Hours • Minutes • Seconds 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 that the server attempts delivery depends on the number of days set in this option.

Table continues…

Name	Description
Report undeliverable mail and delete it after	The number of days after which the system returns an undeliverable message to the sender. The options are: • Days • Hours • Minutes • Seconds When this threshold expires, the sender receives an email that the message is undeliverable. The email includes the original message. 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.

Table continues…

Name	Description
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 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.
Messages in SMTP queue (defer/active/ incoming)	Displays the actual number of messages waiting in the SMTP 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 do the following diagnostics on an installed analog-line interface card:

- Busying out voice channels
- Diagnosing the voice equipment
- Displaying the voice equipment status
- Releasing the voice channels

Related links

Busying out voice channels on page 397
Diagnosing the voice equipment on page 398
Displaying the voice equipment status on page 399
Releasing the voice channels on page 400

Busying out voice channels

About this task

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**.
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 webpage.

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.

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. The valid range is from 0 to 219.

Table continues…

Name	Description
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 click **yes** in the **Immediate Diagnosis** field, the system disconnects all calls that are in progress. Do not click **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.

Name	Description
Equipment to diagnose	Displays the equipment to diagnose as **Card**.
Equipment Number	Administers the number of the card. The valid range is from 0 to 219.
Immediate Diagnosis?	Takes specified channels out of service immediately even if a call is in progress. Click **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

Name	Description
Card	Identifies the circuit card on which the channel resides.

Table continues…

Name	Description
Port	The virtual port number.
Channel	The virtual channel number.
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

About this task

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 webpage.

Release of Voice Equipment field descriptions

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. The valid range is from 0 to 219.

Security

Usage of imported server identity certificates instead of the default identity certificate

Starting from Release 7.1.0, the Messaging server no longer supports the use of the default identity certificate, which is signed by the Avaya Product Root CA. In the previous releases, this certificate was automatically loaded into the Messaging application Identity Certificate stores by the Authentication File Server at the time of installation. Starting from Release 7.1.0, you must import identity certificates into one or more Messaging application trust stores.

To create Messaging Identity Certificates, do one of the following:

- Import certificates that are created and signed by a third-party CA vendor, such as Verisign or Entrust.
- Create and sign the Identity Certificate for Messaging by using the Trust Management PKI feature of Avaya Aura® System Manager.
- Generate a Certificate Signing Request (CSR) by using the Messaging SMI and then send the CSR to a signing authority.

In each of the options, the Messaging SMI directs the download of the Identity Certificate to store it into one or more Messaging application trust stores. These application trust certificates are exchanged during the TLS client or server handshake to securely confirm the identity of the Messaging application.

Generating a certificate signing request

About this task

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) webpage 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.

   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 webpage. You must send the certificate output from the Certificate Signing Request - Display webpage 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 404.

Related links

Certificate Signing Request - Form field descriptions on page 403

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.

Table continues…

Certificate Field	Field Value
Signing Request Hashing Algorithm	Select the hashing algorithm from the drop-down list to sign the certificate.
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

About this task

Use the Download Files webpage to download files onto the Avaya server from another server across the network using HTTP protocol. Typical files to download include new license, 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 webpage, the server must be able to access the:

- Corporate LAN and 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 **Browse** 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 webpage.

   After the system copies the certificates to the `/var/home/ftp/pub` directory, you must install the certificates using the SMI.

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.
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)** > **Miscellaneous** > **Download files**. Browse for the files on your personal computer and load the files to the Messaging server.
2. On the Trusted Certificates webpage, click **Add**.
3. On the Trusted Certificates - Add webpage, 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 webpage 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.

Related links

Adding a server and application certificate on page 409

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 webpage, select a certificate, and click **Copy**.

   SMI displays the Trusted Certificates - Copy webpage 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**.

   While creating the copy, the webpage verifies the following:

   - If the file name is unique and does not already exist.
   - If the copy with a new file name is identical to an existing certificate.

Trusted Certificates field descriptions

Name	Description
Select File	The name of the individual certificate file. The file name is the same in all 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 • **R**: Remote Logging

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)** > **Miscellaneous** > **Download files**. Browse for the files on your personal computer and load the files to the Messaging server.
2. On the Server/Application Certificates webpage, click **Add**.

   The system displays the Messaging certificate file in the `/var/home/ftp/pub` directory with a .pem or .crt extension.
3. On the Server/Application Certificates webpage, 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 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 webpage displays the issued-to, issued by, and date of expiration information for each added certificate in the chain.

   If the file does not contain a valid certificate, the system displays an error message.
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 a single server and application certificate chain, the server subdirectory 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 the system supports only one identity. The system overwrites the existing `server.crt` file.

7. Click **Add**.

   After the successful installation of the server certification, the SSL client, such as the browser of the client computer that gains access to SMI, displays a prompt. After you accept the change, the system displays the webpage that you last visited.

   Note:

   If you fail to install a certificate in one repository, the failure does not affect the installation in other repositories.

8. Restart Messaging.

Next steps

If the certificate fails to load or Messaging displays the `Could not get local issuer` message, troubleshoot the error.

Related links

Stopping Messaging on page 460
Starting Messaging on page 460
Messaging certificate fails to load or displays the Could not get local user message on page 562

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
Select 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.

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

About this task

Use the Server Access webpage 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 **Enable** or **Disable**:
   - SSH Server (SCP/SFTP 22)
   - High Priority SSH (2222)
   - SAT over SSH (5022): Not applicable to Messaging
3. Click **Submit** to save the changes.

Selecting a minimum supported TLS version required to access SMI

About this task

Use this procedure to select a minimum TLS version that is required to access the System Management Interface (SMI). Avaya Aura® Messaging supports the following TLS versions:

- 1.0
- 1.1
- 1.2

Note:

If your browser does not support the configured TLS version, you cannot use SMI.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Server Access**.
2. In the Minimum TLS Versions section, select the required TLS version for the following connection types:
   - **System Management Interface (SMI) pages**
   - **Filesync connections**

   Note:

   Avaya Aura® Messaging does *not* support **CM Duplication Link** and **CM signaling connections**.
3. Click **Submit** to save changes.

Enabling or disabling Avaya Services access using ASG

About this task

Use this procedure to allow or disallow the Avaya support personnel to access your Messaging system using the Access Security Gateway (ASG). Avaya recommends to enable access as it extends the Avaya support capabilities in resolving product issues.

Procedure

1. On the **Administration** menu, click **Server (Maintenance)** > **Security** > **Server Access**.
2. To enable or disable access using ASG, in the **Avaya Services Access via ASG**, click **Enable** or **Disable**.
3. Click **Submit** to save 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 webpage, 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 webpage, verify the access mask 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.

Table continues…

Button	Description
De-select All	To de-select all user-defined access masks listed on the page.
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.

Managing Meltdown and Spectre vulnerabilities

About this task

Avaya Aura® Messaging Release 7.1.0 includes the Red Hat patches to support mitigation of the Meltdown and Spectre vulnerabilities. The choice to enable or disable these patches is a trade-off between performance and security impact:

- If the patches are enabled, the system might experience noticeable performance losses.
- If the patches are disabled, the system is not protected against the Meltdown and Spectre vulnerabilities.

Use the `kernel_opts.sh` kernel configuration script to control how the Meltdown and Spectre vulnerabilities are handled.

For more information about the Meltdown and Spectre vulnerabilities, see https://access.redhat.com/security/vulnerabilities/speculativeexecution.

Procedure

1. Log in to the Avaya Aura® Messaging CLI as an administrator.
2. Run one of the following commands:
   - To review the current status of the kernel options: `kernel_opts.sh status`.
   - To enable the patches to provide maximum protection: `kernel_opts.sh enable`.
   - To disable the patches to provide maximum performance: `kernel_opts.sh disable`.

   Changes made by the script take effect immediately and do not require a server reboot.

Using diagnostic tools

Testing the alarm origination

About this task

Use the Test Alarm Origination webpage 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 webpage.

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**.

Related links

Viewing the alarm logs on page 324

Testing the network connection

About this task

Use the Test Network Connection webpage 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** > **Network Connection**.
2. Select a machine from the drop-down list.
3. Click **Run Test**.

   The system displays the test results.

Testing the SMTP connection

About this task

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 webpage.

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

About this task

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 webpage.

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

About this task

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 webpage.

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

About this task

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 webpage.

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

About this task

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 webpage. 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 webpage.
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 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

About this task

Use the Diagnostics (Application) webpage 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)**.

Related links

Accessing diagnostics results on page 343

Diagnostics (Application) field descriptions

Diagnostic test	Description
All tests	Runs all available tests. Enter at least: • An extension for the **Call-out** test. • A mailbox number or an email address for the **User and Contact Lists** query.
Application Distributed Cache	Tests that the distributed cache server is running and verifies that data can be read, written, and deleted.

Table continues…

Diagnostic test	Description
Call-out	Tests whether outbound calls are established by calling a specific extension. When you pick up the deskphone, you must hear a test greeting. Administer the following parameters: **Use default telephony parameters** — Select this check box to use the default telephony parameters. When you clear this check box, you can customize some of the telephony parameters that SIP uses. **Telephony profile name** — The profile name of the far-end SIP domain that you want the test to use. Far-end SIP domains are added on the Telephony Domains page. If you retain the default value, Messaging automatically selects a telephony profile. **Caller ID name** — The caller ID of the test. **Caller ID number** — The number that the caller ID displays for the test. **P-Asserted Identity name** — The name that you want to enter in the identity information of the P-AI header. **P-Asserted Identity number** — The number that you want to enter in the identity information of the P-AI header. **Port (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 the ADCS' in a cluster to verify if all the ADCS' respond.

Table continues…

Diagnostic test	Description
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 the serial SMDI/MCI integrations, the system also tests the SMDI or MCI link.

Table continues…

Diagnostic test	Description
Fax Outcall	Tests that the application server can send a fax to the specified fax number. You do not need to gain access to a computer system with the outbound fax client software to run this test. Administer the following parameters: **Enable fax diagnostic** — Select this check box to enable the outbound fax diagnostics feature. SMI displays this check box only when you select **All tests** from the **Select the test(s) to run** drop-down list. **Fax number** — The destination fax number. **Use default telephony parameters** — Select this check box to use the default telephony parameters. When you clear this check box, you can customize some of the telephony parameters that SIP uses. **Telephony profile name** — The profile name of the far-end SIP domain that you want the test to use. Far-end SIP domains are added on the Telephony Domains page. If you retain the default value, Messaging automatically selects a telephony profile. **Caller ID name** — The caller ID of the test. **Caller ID number** — The number that the caller ID displays for the test. **P-Asserted Identity name** — The name that you want to enter in the identity information of the P-AI header. **P-Asserted Identity number** — The number that you want to enter in the identity information of the P-AI header. **Fax size** — From the **Select the test(s) to run** drop-down list, if you select

Table continues…

Diagnostic test	Description
	to run only this test, you can choose to send the sample fax transmission in the following different sizes: • Small • Medium • Large To troubleshoot an application server that does not send faxes to the specified numbers, you can enable the detailed logging of errors and use the diagnostic test to send a sample fax.
Messages to Deliver	Queries ADCS through TUI to check the number of messages that the system must 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. Administer the following parameters: **Type of user/ contact list** — The contact list that Messaging searches to find the specified user or contact. 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 find.
Voice Messaging Application	Diagnoses the state of the Messaging application and the communication link to AxC.

Running diagnostic tests on the storage server

About this task

Use the Diagnostics (Storage) page to run one or more diagnostic tests to verify the integration of Messaging with the storage 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.

Before you begin

Ensure that you installed the storage server.

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **Diagnostics (Storage)**.
2. To run:
   - A single test, select a test from the **Single Diagnostic** drop-down list.
   - Multiple tests, select a test from the **Diagnostic Group** drop-down list and select the tests.
3. Click **Run**.

   Messaging performs the selected diagnostic tests and displays the test results.

Diagnostics (Storage) field descriptions

Name	Description
Single Diagnostic	The single diagnostic tests are: • **Show Application servers status**: Displays a list of the active application servers. **Check WNS connectivity with Application servers**: Displays the number of application servers with WNS connectivity.
Diagnostic Group	The group diagnostic tests for: • **MSS Check**: - **LDAP access**: Connects to the LDAP server to determine whether the connection is successful. - **IMAP access**: Connects to the IMAP server to determine whether the connection is successful. This test verifies the internal IMAP port 55413 for the super user. - **SMTP session creation**: Establishes a session to determine whether the SMTP sessions establish successfully. - **Postmaster existence**: Checks whether the postmaster mailbox is configured and available. - **ELA Shadow mailbox existence**: Checks whether the ELA Shadow mailbox is configured and available. If this test fails, you can configure the mailbox on the System Mailboxes page. For more information about creating mailboxes, see *Creating a shadow mailbox*.

Related links

Creating a shadow mailbox on page 72

Running diagnostic tests on ADCS

Procedure

1. On the **Administration** menu, click **Messaging** > **Diagnostics** > **Diagnostics (ADCS)**.
2. To test the ADCS cache of:
   - All users, select a cache from the drop-down list in the **General** section.
   - A specific user, enter the mailbox number of the user, and select a cache from the drop-down list in the **User-Specific** section.

   The options are:
   - **Greetings**
   - **User info**
   - **Voice mails**
   - **All**
3. Click **Diagnose**.

   Messaging displays the diagnostic test results.

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 Results webpage 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.
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.

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.

Table continues…

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

Output type

Name	Description
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

Name	Description
Show numeric addresses	To ensure that the addresses display numerically on the Netstat Results webpage. 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

Name	Description
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. The socket type is AF_UNIX, that is, the local machine socket. You can view the results for inet, inet6, and UNIX address families on the same page, by selecting 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.
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.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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

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) webpage.

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 affect the 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
Cluster Hit Rates	
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.
Storage Backend Hits (storage servers)	The percentage of times the system made a request and found the required data in the storage 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 write to a cache but failed.
Storage Usage	
Storage usage	The percentage of the local and the cluster storage used.
Storage quota	The total capacity of the local and the cluster storage.
Cache Contents	
Number of unsynced messages	The total number of unsynchronized messages in the cache.
Counters	
Last cleared	The date and time when the cache statistics were last reset. Click **Clear counters** to reset the cache statistics.

Advanced application server settings

Reload application server cache

Use the Reload Caches panel to force cache reloads. During normal operations, you do not need to do manual reloads of the data caches for the application server. 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 the following situations:

- Force a manual reload of **User List**, **Global Address List**, **System Greeting**, or **Classes of service** if network problems have impaired communications between AxC and the

application server. For example, reload caches if you changed the extensions of local users or caller applications.

The time taken to reload GAL depends on the size of the list and the responsiveness of 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 file is updated on the AxC server.
- Force a reload of the Classes of Service definition file if the file is updated on the AxC server.
- Force a synchronization of the Distributed Cache if the application server is offline for a long period.

  The application server synchronizes the data with the associated AxC server.

System Operations field descriptions

Reload Caches

Name	Description
User List	The option to reload User List.
Global Address List	The option to reload Global Address List.
System Greeting	The option to reload the system greeting.
Classes Of Service	The option to reload the CoS.
Application Distributed Cache (ADCS)	To option to synchronize ADCS.

System Operations Advanced

Name	Description
Restart Voice Messaging Application	The option to restart the voice messaging application.
Restart Voice Browser	The option to restart the voice browser.
Restart Text-To-Speech engine	The option to restart the Text-To-Speech engine.
Restart ADCS	The option to restart ADCS.
Restart Web Access	The option to restart the Messaging Web Access server.

Local Directory Cache

Name	Description
Clear the local directory cache (excludes ADCS)	The option to clear the local directory cache.

Distributed Cache (ADCS) Maintenance

Name	Description
General	

Table continues…

Name	Description
Delete ADCS cache directory and restart ADCS, Voice Messaging Application and Web Access	The option to delete the ADCS cache directory and restart ADCS, Voice Messaging Application, and Web Access. The system deletes the system configuration and user information from the cache. The system deletes undelivered login announcement 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	The option to clear all data in the ADCS cache on this application server. 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	The option to remove any recorded greeting or name inconsistencies in the cache between the application and storage servers. 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

Name	Description
Clear a user's data in ADCS cache on this application server	
User's mailbox	The mailbox number of the user.
Types of objects to delete	The option to delete the type of objects. 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

Communication with AxC

Name	Description
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.
Storage Synchronizer retry period	The storage synchronizer retry period in minutes.
Storage Synchronizer retry attempts	The retry attempts for the storage synchronizer.
Storage Synchronizer connection timeout	The storage 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

Name	Description
ADCS communication timeout	The ADCS communication time-out in milliseconds.
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

Name	Description
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.

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. The 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 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 in this 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.

Enabling core file generation

About this task

Use the Core Files webpage 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

IPv6

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

In December 1998, the Internet Engineering Task Force published RFC 2460, the internet standard specification that defines IPv6.

Addressing

By using 128–bit addresses, IPv6 has about $3.4x10^{38}$ unique IP addresses, more than enough for every network device. This eliminates the IPv4 mechanisms, such as NAT, that are used to relieve IP address exhaustion. IPv6 addresses are normally written as hexadecimal digits with colon separators, for example, 2005:af0c:168d::752e:375:4020. The double colon "::" represents a string of zeroes according to RFC 4291.

Simplification

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

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

Deployment and transition

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

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

Key differences between IPv4 and IPv6

Parameter	IPv4	IPv6
Address space	32–bit, about $4.3x10^{9}$	128–bit, about $3.4x10^{38}$
Security	IPSec support is optional.	IPSec support is required.
Configuration	DHCP or manual configuration required.	Stateless auto-configuration. Does not require DHCP or manual configuration.
Address format	Decimal digits with colon separators, for example:192.168.1.1	Hexadecimal digits with colon separators. For example: 2005:af0c:168d::752e:375:4020. The double colon"::" represents four zeroes "0000".
Broadcast and Multicast support	Yes	No Broadcast. Various forms of Multicast-better network bandwidth efficiency.
QoS support	ToS using DIFFServ	Flow labels and flow classes, more granular approach.

Enabling IPv6

Procedure

1. Log in to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
3. In the **IPv6 is currently** field, click **enabled**.
4. Click **Change**.
5. Reboot Messaging.

Disabling IPv6

Procedure

1. Log in to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
3. In the **IPv6 is currently** field, click **disabled**.
4. Reboot Messaging.

Configuring additional network settings

About this task

Perform this procedure only if you are deploying the Avaya Aura® Messaging OVA using the vSphere Client or the vSphere Web Client that is directly connected to the ESXi host.

Note:

If you are deploying the Avaya Aura® Messaging OVA using the vSphere Client connected to vCenter, the system prompts you to specify network parameters during the deployment process.

Use the Network Configuration webpage to configure or view the settings for the:

- Host name
- DNS domain name
- DNS search list
- DNS IP addresses
- Server ID
- Default gateway

Procedure

1. Log in to the Messaging System Management Interface.
2. In the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
3. Click **Continue** at the warning.
4. Enter the appropriate information in the fields.

   If IPv6 is not enabled, you cannot configure the IPv6 fields.
5. Click **Change**.

Related links

Network Configuration field descriptions on page 449

Network Configuration field descriptions

Name	Description
Host Name	The host name of the Messaging system. The host name must be unique.
DNS Domain	The DNS domain name of the server. For example, company.com. **Note:** To ensure that Internet Messaging works properly, you must enter the Fully Qualified Domain Name (FQDN) of the server.
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. This field is currently not in use.
IPv6 is currently	The specific status of IPv6. The options are: • **enabled** • **disabled**
Default Gateway IPV4	The default gateway address of IP version 4. If the server supports the IPv6 network, in the IPv6 area, enter or view the default gateway address of IP version 6.
Default Gateway IPV6	The IPv6–compliant IP address of the default gateway.
IP Configuration	The set of parameters to configure an Ethernet port such as eth0, or eth1. The parameters are: • **IPv4 Address** • **Mask** • **IPv6 Address** • **Prefix**

Table continues…

Name	Description
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 the short version and long version of the mask. If you are using the short version, enter a number from 1 to 32.
Functional Assignment	Based on the system configuration, the system displays the following options: • Corporate LAN/Processor Ethernet/Control Network • Corporate LAN/Control Network • Out-of-Band Management

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 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 webpage, 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.
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.

Server maintenance

Changing the IP addresses and host names of a single-server on VMware

About this task

Perform these steps on the Messaging SMI.

Procedure

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
3. Change the relevant IP addresses and the host names, such as Host name, DNS Domain, Primary DNS, Default Gateway IPv4, IPv6, IP Configuration, and click **Change**.

While changing the IP address, do not reboot the server or activate the Start or Stop action of Messaging for changing the host name.

4. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**.
5. In the **Add Application Server** section:
   a. Enter the new IP address.
   b. Select **The same site configuration as an existing application server**
6. Click **Add**.
7. In the **Sites / Application Servers** section, change the status of the IP address of the old application server to Inactive and click **Update**.
8. In the **Remove Application Server** section, select the IP address of the old application server and click **Remove**.
9. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Shutdown Server**.
10. On the Shutdown Server webpage, select **Delayed Shutdown**.
11. Select the **Restart server after shutdown** check box.
12. Click **Shutdown**.

    The system displays the confirmation screen.
13. Click **OK** to continue.
14. Log in to the Messaging SMI and, on the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**, and in the **Sites / Application Servers** section, ensure that status of the new application server is **Active**.

Next steps

Depending on your network requirements, you might need to also change the Messaging IP addresses on the following SMI webpages:

- Telephony Integration
- External Hosts
- Trusted Servers
- Network servers
- Mail Options
- Miscellaneous

Related links

Logging in to Messaging on page 37
Adding additional application servers on page 132
Stopping Messaging on page 460
Starting Messaging on page 460

Changing the IP addresses and host names of application servers on VMware

Procedure

1. Log in to the Messaging SMI from the storage server.
2. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**.
3. In the **Sites / Application Server** section, change the status of the IP address of the old application server to Inactive, and click **Update**.
4. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
5. Click **Continue** at the warning.
6. Change the relevant IP addresses and the host names, such as Host name, DNS Domain, Primary DNS, Default Gateway IPV4, IP Configuration.

   While changing the IP address, do not reboot the server or activate the Start or Stop action of Messaging for changing the host name.
7. Click **Change**.
8. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Shutdown Server**.
9. On the Shutdown Server webpage, select **Delayed Shutdown**.
10. Select the **Restart server after shutdown** check box.
11. Click **Shutdown**.

    The system displays the confirmation screen.
12. Click **OK** to continue.

    Note:

    Repeat the Step 1 to Step 12 for each application server with the new IP addresses before moving to the next steps.
13. Log in to the Messaging SMI from the storage server.
14. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**.
15. In the **Add Application Server** section:
    a. Enter the new IP address.
    b. For the first application server, select **No active site configuration**.

       For subsequent application servers, select **The same site configuration as an existing application server**.

16. Click **Add**.
17. In the **Remove Application Server** section, select the IP address of the old application server, and click **Remove**.
18. If an application server is in cluster, then to change the cluster configuration on all cluster members, click **Server Settings (Application)** > **Cluster** and change the IP addresses of the cluster members.
19. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**, and in the **Sites / Application Servers** section, change the status of the new application server to **Active**.

Related links

Network Configuration field descriptions on page 449

Changing the IP address of the Avaya message store on VMware

Procedure

1. Log in to the Messaging SMI from the application server.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
3. Click **Continue** at the warning.
4. Change the relevant IP addresses and the host names, such as Host name, DNS Domain, Primary DNS, Default Gateway IPV4, IPv6, and IP Configuration.
5. Click **Change**.
6. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Shutdown Server**.
7. On the Shutdown Server webpage, select **Delayed Shutdown**.
8. Select the **Restart server after shutdown** check box.
9. Click **Shutdown**.

   The system displays the confirmation screen.
10. Click **OK** to continue.
11. Log in to the Messaging SMI from the application server.
12. On the **Administration** menu, click **Messaging** > **Server Settings** > **Server Role / AxC Address**, and change the **AxC IP address**, and click **Apply**.

    Ensure that you change the **AxC IP address** for all application servers.

Related links

Network Configuration field descriptions on page 449

Server shutdown

Purpose

Use the Shutdown Server Web page to shut down the server. 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 secondary server. The selection also affects the method in which the secondary 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 could result 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. Log on to Messaging System Management Interface.
2. In the **Administration** menu, click **Server (Maintenance)** > **Server** > **Shutdown Server**.

3. On the Shutdown Server webpage, select from the following options:
   - **Delayed Shutdown**
   - **Immediate Shutdown**
4. **(Optional)** Select the **Restart server after shutdown** check box.
5. Click **Shutdown**.

   The system displays the confirmation screen.
6. 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.

   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.

Related links

Changing the configuration of a cluster on page 184
Topology field descriptions on page 145

Restarting the server

About this task

Use this procedure to restart the server after stopping the Messaging software.

Procedure

1. Log in to the Messaging System Management interface.
2. On the **Administration** menu, click **Messaging** > **Utilities** > **Stop Messaging**.

3. Click **Stop**.

   The system delays the shutdown process until all calls are completed. However, after three minutes, the system terminates all active calls.

   The Stop Messaging Software webpage refreshes periodically during the shutdown process and displays the relevant status message.

   After the Messaging software stops, the system displays the following message:

   ```
   Stop of Messaging completed.
   ```

4. Click **OK**.

   The system stops the Messaging software before you restart the server.

Note:

Restarting the server without stopping the Messaging software might corrupt the database.

5. On the **Administration** menu, click **Server (Maintenance)** > **Server** > **Shutdown Server**.
6. On the Shutdown Server webpage, select one from the following :
   - **Delayed Shutdown**
   - **Immediate Shutdown**
7. Select the **Restart server after shutdown** check box.
8. Click **Shutdown**.
9. Click **Ok**.

Restarting Messaging Web Access

Procedure

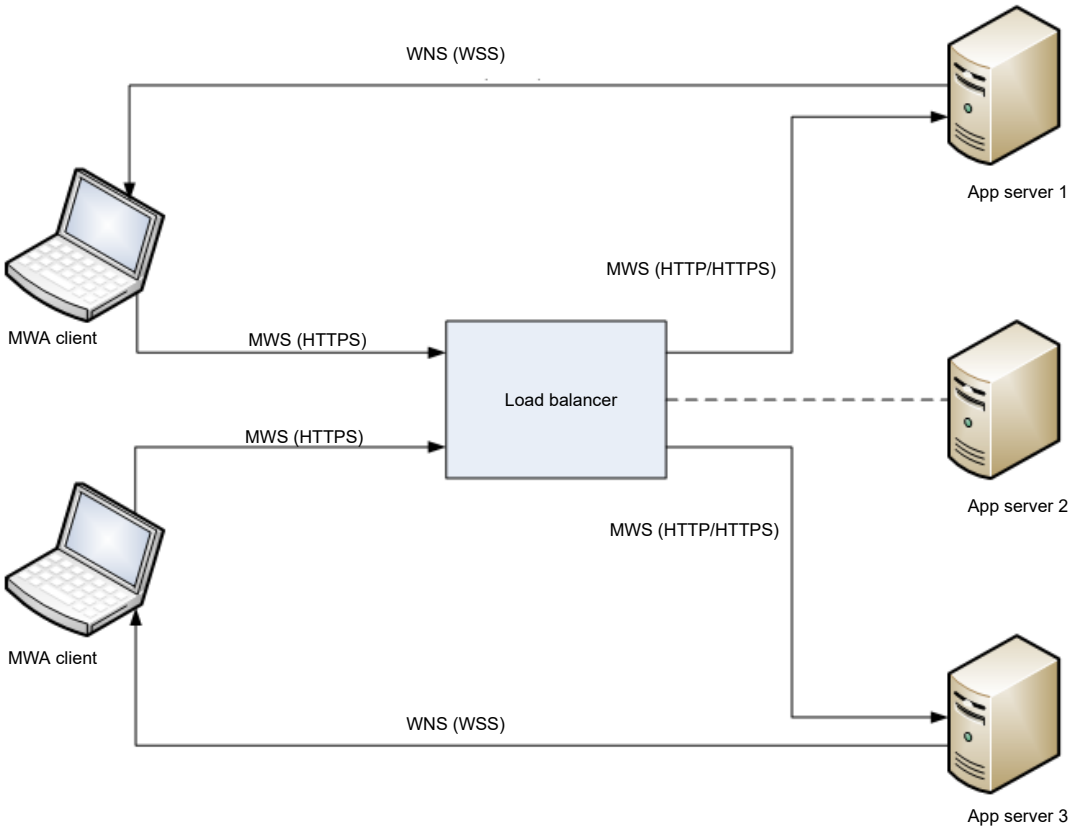
1. On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**.
2. In the **System Operations Advanced** section, next to **Restart Web Access**, click **Restart**.

   Messaging restarts Messaging Web Access.

Load balancing Messaging Web Access

Deploy a load balancer before the Messaging Web Access system to achieve the following:

- Distribute the client load evenly among application servers.
- Maintain service availability when an application server becomes unreachable or goes offline.
- Provide a single URL instead of multiple application server URLs to clients.



A client communicates with an application server using the following protocols:

- Messaging Web Service (MWS) over HTTPS.
- Web Notification Service (WNS) over secure WebSocket.

A load balancer distributes MWS requests. When a client sends a request to a particular application server, the application server establishes a WNS connection with the client.

A load balancer must support the following:

- Operation at layer 7, that is HTTP.
- Sticky sessions, which indicate that all HTTP requests from a single client session must go to the same application server. This happens when the load balancer inserts a cookie in the client to record the choice of application server in the response to the first request.

Note:

The network design must enable direct WebSocket connections between clients and application servers. The WebSocket connections start off as HTTP.

Important:

If the network connecting the load balancer to the application servers is secure, the system administrator can choose between HTTP and HTTPS to run the MWS. Running the MWS over HTTP reduces the load. However, for the network connecting a client and the load balancer, the system administrator must always run the MWS over HTTPS.

Restarting Messaging

Stopping Messaging

About this task

Use the Stop Messaging Software webpage to stop the Messaging software.

Procedure

1. Log in to Messaging System Management Interface.
2. In the **Administration** menu, click **Messaging** > **Utilities** > **Stop Messaging**.

   The system displays the Stop Messaging Software webpage.
3. 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 webpage 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.
4. Click **OK**.

Starting Messaging

About this task

Use the Start Messaging Software webpage to start the Messaging software.

Procedure

1. Log on to Messaging System Management Interface.
2. In the **Administration** menu, click **Messaging** > **Utilities** > **Start Messaging**.

   The system displays the Start Messaging Software webpage. This webpage 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.
3. Click **OK**.

Manage updates

Use the Manage Updates webpage to manage updates. The types of updates include service pack, security service pack, and kernel 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 webpage, 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: • **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.

Table continues…

Name	Description
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 set the number.

Table continues…

Name	Description
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. • **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**

Table continues…

Name	Description
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. 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 webpage.

2. In the **Content** area, click **Summary** or **Detailed**.
3. In the **Frequency** area, click **Display once** or **Refresh page every __ seconds**.
4. To display the process status of all server applications, click **View**.

   The system displays the Process Status Results webpage.

Related links

[Process Status field descriptions](#) on page 465

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 webpage displays the status information for server applications based on the selections you make in Viewing the process status on page 464.

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.
CMFPAgent	Handles SNMP requests for objects defined in the CMFP.
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].

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, 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.

Table continues…

Name	Description
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 *100,000* or higher, the higher the better and virtual memory must be below *200,000*, 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.

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

Table continues…

Storage server	Application server	Experience
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
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: Migration

Migrating Avaya CallPilot® Subscriber Data

Avaya CallPilot® migration overview

Messaging supports the migration of subscriber data and media from Avaya CallPilot® Releases 4.0, 5.0, and 5.1. The migration process consists of two phases:

- Exporting the CallPilot® data using CallPilot® export tool.
- Importing the CallPilot® data using Messaging System Management Interface by selecting and uploading an archive that contains the CallPilot® data.

Planning and preconfiguration

Pre migration requirements

Best practice

For a successful migration, implement the following best practices:

- Identify a server with adequate disk space to store the data sets. The Messaging server backs up the Messaging data through the customer LAN to an external server. The network must support a minimum average transfer rate of 1.6 MB/sec. The supported backup methods are SFTP and SCP.
- Verify that you have the required applications on the computer to perform the migration.
- Ensure that you have a monitor, a mouse, and an appropriate keyboard to connect to the server.

Application requirements

Performance Enhancement Package (PEP). In this document, CallPilot® Export Tool refers to PEP.

Archive storage

Use an externally attached or a network-accessible storage device to store the archived files.

List of migrated attributes

The following list describes the mapping between the attributes of CallPilot® and Messaging.

Attributes present on both systems

CallPilot®	Messaging	Notes
Last Name	**Last name**	Messaging supports maximum 27 characters for the **Display name** attribute, which includes **First Name** and **Last Name**. If the combined value exceeds 27 characters, the migration tool truncates **First Name**.
First Name	**First name**	Messaging supports maximum 27 characters for the **Display name** attribute, which includes **First Name** and **Last Name**. If the combined value exceeds 27 characters, the migration tool truncates **First Name**.
Mailbox Number	**Mailbox Number**	The length of the mailbox number must be the same on the CallPilot® system and the Messaging system.
Extension DNs	• **Extension** • **Additional extensions**	Messaging migrates: • **Extension DN 1** to **Extension**. • **Extension DN 2**, **Extension DN 3**, **Extension DN 4**, **Extension DN 5**, **Extension DN 6**, **Extension DN 7**, **Extension DN 8** to **Additional extensions**. Messaging does not import the subscriber data of the CallPilot® users who do not have an extension number.
Location Name	**Site**	**Location name** on the CallPilot® system is **Site** on the Messaging system. On Messaging, you must configure **Site** with the **Location Name** in CallPilot®. **Note:** The name comparison between the two systems is not case sensitive. If a site with the same name is nonexistent in the Messaging system, the tool migrates the mailboxes from the CallPilot® system to the default site with ID 1 on the Messaging system. **Important:** For the CallPilot® data to work correctly in Messaging, the mailbox number length and the short mailbox length administered in Messaging must match the mailbox length administered for the subscribers that you migrate from CallPilot®.
Language	**Language**	You must install required language packs on the Messaging system before migration. If any language is nonexistent in the Messaging system, the tool migrates the mailboxes from the CallPilot® system to the default language on the Messaging system.
Time Zone	**Time Zone**	—

Table continues…

CallPilot®	Messaging	Notes
MWI DNs	**MWI enabled**	The Messaging system enables MWI if MWI DN and the mailbox number are the same and the MWI DN is enabled on the CallPilot® system.
Mailbox Class	**Class Of Service**	**Mailbox Class** on the CallPilot® system is **Class Of Service** on the Messaging system. You must configure **Class Of Service** on the Messaging system with the same **Mailbox Class** name as in the CallPilot® system. **Note:** The name comparison between the two system is not case sensitive. If a **Class Of Service** with the same name is nonexistent in the Messaging system, the tool migrates the mailboxes from the CallPilot® system to the default **Class Of Service** with ID 0 on the Messaging system.
PDL	**PDL**	The migration tool migrates only **Local User addresses** and skips all other addresses. PDL number on the Messaging system is CallPilot® PDL number + 10. As a result, the migration tool migrates CallPilot® PDL numbers that are less than 90. Messaging adds a number as a suffix to PDLs with identical names for one mailbox. For example, Messaging changes the name of 2 PDLs with the MyPDL name to MyPDL and MyPDL(1).
Greetings	**Greetings**	The migration tool migrates external greetings to the Messaging system. The following is the Greetings migration schema. The Greeting migration schema includes: • Temporary Absence Greeting-Extended Absence • External Personal Greeting-Personal No Answer • Personal Verification-Name Recording • Temporary Absence Greeting Expiry-EAG Expiration Time **Note:** If external greeting is not recorded and internal greeting is recorded, the migration tool uses the internal greeting as the personal greeting. If both external and internal greetings are recorded, then the migration tool migrates the internal greeting as the optional greeting #1, to all internal callers.
Operator/Revert DN	**Operator**	The operator number must comply with Dial Rules for **Class Of Service** on the Messaging system.

Attributes present on both systems with features imported from CallPilot®

CallPilot®	Messaging	Notes
Block Incoming Messages	**Block Incoming Messages**	—
Auto-logons flags for extensions	**Allow auto login**	Messaging does not import the subscriber data of the CallPilot® users who have the same extension number administered in **Auto-logons flags for extensions** and **Multiple Remote Notification Targets**.
Multiple Remote Notification Targets	**Notify Me settings**	Messaging imports: • The first phone number • The email addresses If a CallPilot® user has multiple email addresses, Messaging imports a maximum of five email addresses, and records a warning for this event in the import log. • An urgent flag for the target phone. • An urgent flag for the email notification. In a voice mail with multiple recipients, if the important flag is not set for all the CallPilot® users, Messaging clears the flag during the migration of the user data. Messaging does not import: • The subscriber data of the CallPilot® users who have the same extension number administered in **Auto-logons flags for extensions** and **Multiple Remote Notification Targets**. • The pager targets.

Attributes present only on the Messaging system

Messaging attribute	Notes
Display name	The attribute is a concatenation of the first name and the last name. (first+" "+last)
ASCII name	The attribute is a concatenation of the last name and the first name. (Last name+","+" "+First name)
Email address	The email address of the mailbox of the user. The attribute is concatenation of the First name, the Last name, and Messaging server FQDN. (First name+"."+Last name+"@"+FQDN)
Numeric address	This attribute is the same as the Mailbox number.
Include in Auto Attendant directory	The attribute is enable.

Table continues…

Messaging attribute	Notes
Password	After the CallPilot migration to Avaya Aura® Messaging, the user can log into Messaging using the CallPilot migrated password only once. You must change the Callpilot migrated password to a new password that complies with the Avaya Aura® Messaging policy settings.

Pre migration data gathering

For successful migration, gather the following data for both systems: CallPilot® and Messaging.

CallPilot®	Messaging	Notes
Location Name	**Site**	• Record the currently configured locations on the CallPilot® system. • Record the currently configured sites on the Messaging system. **Note:** **Location name** on the CallPilot® system is **Site** on the Messaging system.
Language	**Language**	Record the currently installed languages on the CallPilot® system and the Messaging system.
Time Zone	**Time Zone**	Record the currently configured time zone on the CallPilot® system and the Messaging system.
Mailbox Class	**Class Of Service**	• Record the currently configured Mailbox Class on the CallPilot® system. • Record the currently configured Class of Service on the Messaging system. **Note:** **Mailbox Class** on the CallPilot® system is **Class Of Service** on the Messaging system.

Pre migration checklist

#	Task	References	Notes	✔
1	Gather pre migration data.	See Pre-migration data gathering on page 476.	—	
2	Back up the CallPilot®system files.	See the Avaya CallPilot® documentation.	—	
3	Back up the Messaging system files.	See Backing up the system on page 284.	—	

Table continues…

#	Task	References	Notes	✔
4	Configure all necessary sites on the Messaging system.	See Overview for administering sites on page 122.	You must configure **Site** on the Messaging system with the same **Location Name** as in the CallPilot® system. **Note:** The name comparison between the two systems is not case sensitive.	
5	Change the mailbox number length.	See Setting the length of the mailbox number on page 69.	The mailbox number length administered in Messaging must match the mailbox number length administered for the subscribers that you migrate from CallPilot®.	
6	Change the short extension length.	See Adding additional sites on page 126.	The short mailbox length administered in Messaging must match the short mailbox length administered for the subscribers that you migrate from CallPilot®.	
7	Install the required language packs on the Messaging system.	See Configuring languages on page 115.	—	
8	Configure all necessary Class of Service on the Messaging system.	See Adding a Class of Service on page 214.	You must configure **Class Of Service** on the Messaging system with the same **Mailbox Class** name as in the CallPilot® system. **Note:** The name comparison between the two systems is not case sensitive.	

Exporting the CallPilot® subscriber data

Installing the CallPilot® export tool

Procedure

1. After you log on, the Setup Wizard opens automatically. Click **Next** on the Welcome page of the Setup Wizard.

2. In the Service Update (SU)/PEP Installation page, select **Yes, I have updates that I want to install now**.
3. Click **Next**.

   The system displays a message prompting you to install SUs and PEPs.
4. Browse to the PEP CD-ROM in the DVD-ROM drive. Review the readme file for important steps required for the PEP or SU.
5. To install an SU or PEP, double-click **cp2msg.msi**.

   The system displays a confirmation message.
6. Click **Yes** to continue.

   Note:

   The system displays the message to restart the server. If the system restarts, log back in to the system. If the Setup Wizard does not open automatically, select **Start** > **programs** > **CallPilot** > **Setup Wizard**.
7. On the Setup Wizard Welcome screen, click **Next**.
8. On the Service Update (SU)/PEP Installation page, select **No, I do not have updates that I want to install now**.
9. Click **Next**.
10. On the Platform Validity page, check that the values listed are correct and marked with green check marks. Click **Next**.
11. On the Telephony Board Validation page, click **Next**.
12. On the Upgrade of CallPilot page, click **No, I do not have data to restore**.
13. Click **Finish**.

Exporting the CallPilot® subscriber data

Procedure

1. Click **Start** > **Run**.
2. In the **Open:** field, enter `cmd`.
3. Navigate to the directory, where you installed the export tool. Enter `cd D:\cp2msg`.
4. In the Command Prompt window, enter `CP2MSG` *`password output_file[OPTIONS]`*`:-range"MBNUM-MBNUM[;MBNUM-MBNUM]" –type TYPE –size SIZE –admin MBNUM –location ID` where:

   - *password* for administrative user with mailbox `000000`.
   - *output_file* is a full path to the folder for resulting archive. Use only externally attached or network mounted storage.

For example, `D:\cp2msg>CP2MSG 123123 X:\Lab\TempDir \CPUsersMigrationTest`. In this example, 123123 is the password and X:\Lab \TempDir\CPUsersMigrationTest is the full path to the folder for resulting archive.

- *range* for mailboxes that need to be exported. You can specify a range separated by semicolons and define range by 2 values that are separated with dash ('-'). The number of digits in the range value must be the same and the first value should not be greater than the second value. When you migrate several ranges, the ranges must be specified in quotes and separated by semicolon. For example, "2000-2005;2008-2010".
- *type*: for the type of data to export. By default all data is exported. Available values are:
  - all
  - profile
  - greetings
  - messages
  - pdls

  When you set a type, then only the items related to the type are included into the XML. Mailbox tag is always included.
- *size* is size of archive parts split in megabytes. Default is 500.
- *admin* is used if the password for 000000 mailbox is not known or the mailbox number is changed.
- *location* is id of the location that can be defined by the exported data. The files in archive are in the format <locationId>_<mailboxNumber>. If the location id is specified, the LDAP is changed accordingly.

For example, `Select x:\test\11\callpilot\users\cp \2_60000.cpuser...valid.` In this example, the string means that a user belongs to a location with ID2.

If you run the export tool under remote non-console session, the system displays the following message: `Error! You are currently logged on to a CallPilot server through a remote desktop virtual connection.`

Importing the CallPilot® subscriber data

Uploading the CallPilot® data

About this task

Upload entire archives or parts of the CallPilot® data.

Before you begin

Ensure that:

- Messaging is running.
- No other data upload is running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **CallPilot Migration**.
2. Click **Browse** and select the CallPilot® archive that you want to upload.
3. To upload:
   - An archive, click **Upload archive**.

     Messaging uploads the CallPilot® data.

     Note:

     Use the **Upload archive** option only if the data archive contains one file.
   - Parts, click **Upload part** and perform the next step.

     Messaging displays the uploaded parts in the list of parts.
4. Click **Join parts** to join the parts of the archive.

   Messaging joins the parts into an archive and displays the archive in the list of archives.

Importing the CallPilot® data

About this task

Import the CallPilot® data using the craft login on the Messaging upload files screen.

Messaging performs the following two tasks when importing the CallPilot® data:

- Imports local user data and greetings and, using the user attributes in the imported data, creates users.
- Imports distribution lists and messages.

Before you begin

Ensure that:

- Messaging is running.
- Another data import is not running.

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **CallPilot Migration**.
2. Select the CallPilot® archive that you want to import.
3. Click **Import**.

   Messaging displays the Import CallPilot Data page.

4. On the Import CallPilot Data page, in the **Import parameters** section, click the appropriate options.
5. Click **Run**.

   Messaging imports the CallPilot® data.

   Note:

   Messaging imports local users only.

- If the CallPilot® data import fails for some users, verify the administration of the users or delete the users using the log files and run the data import again.
- Messaging does not import the subscriber data of the CallPilot® users:
  - Who do not have an extension number administered to the mailbox.
  - Who have the same extension number administered in **Auto-logons flags for extensions** and **Multiple Remote Notification Targets**. These fields map to **Allow auto login** and **Notify Me settings** in Messaging.
  - Whose short extension length and short mailbox length is shorter than the lengths administered in the Messaging site, if Messaging has only the **Default** site administered.
  - Whose mailbox numbers contain the same sequence of digits as the digits of the CallPilot® password. The mailbox numbers might contain all or part of the digits of the CallPilot® password.

Next steps

View the log files of the CallPilot® data import.

Import parameters field descriptions

Name	Description
Data to import	To import a particular data type. The options are: • **All** • **Profile** • **Greetings/Name** • **Messages** • **PDLs** Default is all. When you select a data type such as Greetings, Messages, or PDLs, the data is migrated only for an existing user with a mailbox number.

Table continues…

Name	Description
Overwrite existing data	To restore data from an archive. By default, this option is cleared. When **Overwrite existing data** is not selected, the system skips overwriting the following data types: • User with matched mailbox number • Greetings of matched type • Messages with matched IDs • PDLs with matched IDs When **Overwrite existing data** is selected, the system updates the following data types: • Profile for user with specified mailbox number • Greetings/Name • Messages with the same message ID • PDLs with specified IDs
Mailbox range (optional)	To specify the range of the mailboxes that need to be exported. Mailboxes within the specified range are processed. By default, the field is empty. When the field is empty, all the mailboxes from the archive are processed.
Apply number prefix modification	To change the mailbox or extensions during migration or both. When you select this **Apply number prefix modification** field, the system enables the related parameters.
Modification type	To add or delete a prefix to or from a number. The options are: • **Add** • **Delete**
Apply to	To define the specific numbers with the following options: • **Mailbox numbers only** • **Extensions only** • **Mailbox numbers and extensions** **Note:** When the import type is PDLs, greetings, and messages, then only mailboxes are modified.
Length	To apply prefix modification to numbers of a specific length. The numeric value must be from 1 to 30.

Table continues…

Name	Description
Prefix	To add or delete a digital prefix. The delete operation takes place only if a number of a specific type has: • A specific length • A specific prefix
Migrate to specific site	To specify a site for imported users. By default, this option is cleared and the users are migrated to the sites that match the location names on CallPilot. The system enables this option only if the profile is set to All or Profile.
Include in Auto Attendant directory	To include the imported users in Auto Attendant directory. By default this option is enabled. The system enables this option only if the **Data to import** is set to All or Profile.

Viewing the logs of the CallPilot® data import

About this task

The beginning of the log contains information about the creation of users, while the latter part contains information about the import of the distribution lists and the messages.

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **CallPilot Migration**.
2. Select the CallPilot® log of the data import that you want to view.
3. Click one of the following:
   - **View** to view the log on the browser.
   - **Download** to download the log to your computer.

   Messaging displays the log files.
   - If you do not import the CallPilot® data, Messaging displays the following message:

     ```
     No log file found
     ```
   - If you do not create a Mailbox COS, import logs contain the following message:

     ```
     Class Of Service <Mailbox class name> is not configured in the system. Using default
     ```
   - If you do not create a site that matches the location name, import logs contain the following message:

     ```
     Site <Location name> does not exist in the system, leaving default
     ```
4. Click **Delete** to delete the selected log file.

CallPilot® Migration field descriptions

Name	Description
CallPilot data file	The CallPilot® archive to import.
Log file	The logs of the data import process.

Button	Description
Import	To import the CallPilot® archive.
View logs	To view the logs of the data import process.

Viewing the results of the CallPilot® data import

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **CallPilot Migration**.
2. Select the CallPilot® result of the data import that you want to view.
3. To view the result of the data import, click **View**.

   Messaging displays the result.

Deleting the CallPilot® data

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **CallPilot Migration**.
2. Select the CallPilot® result of the data import that you want to delete.
3. To delete the selected import log or import result, click **Delete**.
4. To delete subscribers imported in the data import, click **Delete subscribers**.

   Messaging displays the Delete Imported CallPilot Subscribers page.
5. To confirm deletion of the imported subscribers, click **Delete**.

Octel Aria

Octel Aria migration

Messaging 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
- Nondelivery notifications
- Passwords
- Multilingual capabilities of the Aria server

Ensure that there are enough 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

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 character except _. For example, `Octel_NAG_stormy92000-92999.zip`.

  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, to change the mailbox number from 92000 to 8888892000, you must provide a mapping file with the name `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.

About this task

Avaya Professional Services must import the Octel Aria data using the *craft* login.

During a migration, Messaging does not save the pending Outcall notices of users with mailboxes on Exchange Server.

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. To view the logs of the import after the import is complete, select 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.

Chapter 20: 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 Mirror caveats

Message Mirror has the following caveats:

- The Avaya message store server and the Message Mirror server synchronize with an NTP server. Use the NTP server in your network to synchronize the time.
- Message Mirror increases the maximum mailbox and the message size on the backup server by 5% while copying the CoS information. With the increase in these sizes, Message Mirror can copy voice messages of the maximum length on the primary server to the backup server.
- You must restart Messaging Web Access every time the system fails over to the backup Message Mirror server or fails back to the primary server.
- Message Mirror *only* replicates user data, except PDLs and ELA members, that you administer in User Preferences and on the following SMI pages:
  - Class of Service
  - User Management

- Users

Messaging does not support Message Mirror when:

- An Exchange Server is the message store
- The user deletes the mailbox in backup storage

Single Server configuration

The simplest implementation of Messaging is the single-server, single-site configuration in which a single virtual server performs the application role and the storage role. The single-server configuration is an ideal solution only as a small, nonredundant Messaging deployment. The configuration can support the requirements of organizations with up to 6000 users. The configuration works well in distributed organizations, as the configuration supports scalability to accommodate organizational growth.

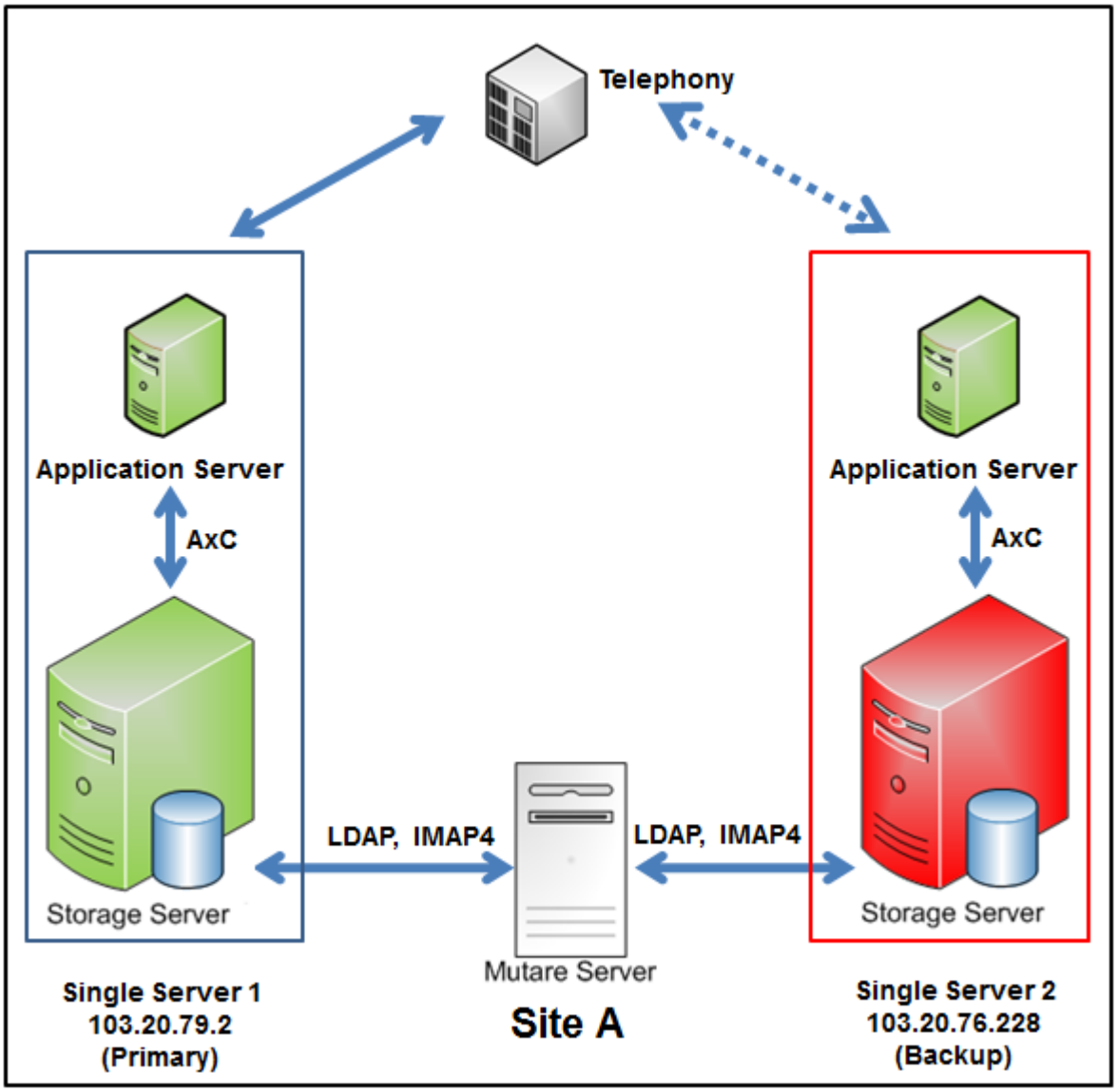
If the number of users at the main site is lesser than the number that the configuration supports, you can use this configuration to add additional application servers at remote office locations. You can also expand your single-server configuration to other Messaging configurations. For example, you might have 2000 users at your main site and a few hundred users at each of several remote locations. In this case, you can add remote users either by administering application servers at those locations or by connecting those users to other sites over a WAN. With this kind of a distributed configuration, you can administer Messaging to support up to 6000 users in your organization.

The following diagram shows the high-level topology for configuring a mirrored single server for message store redundancy. 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 Server configuration

In this configuration, the primary storage server and the backup storage server reside at two different sites.

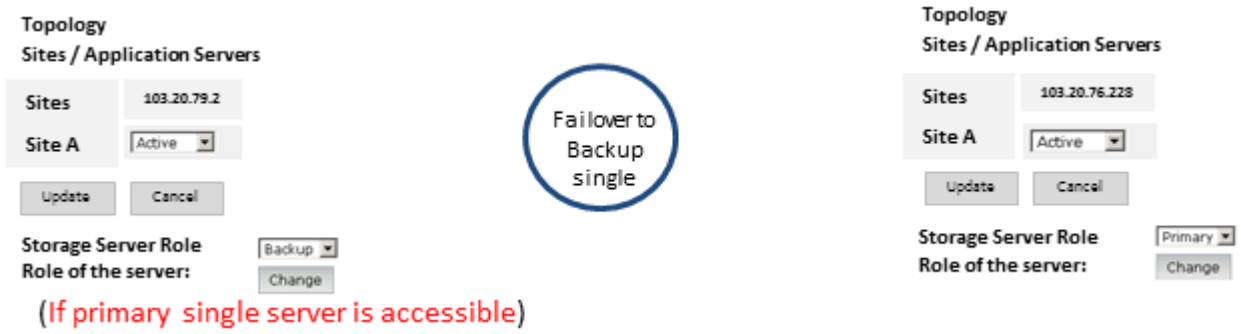


Example

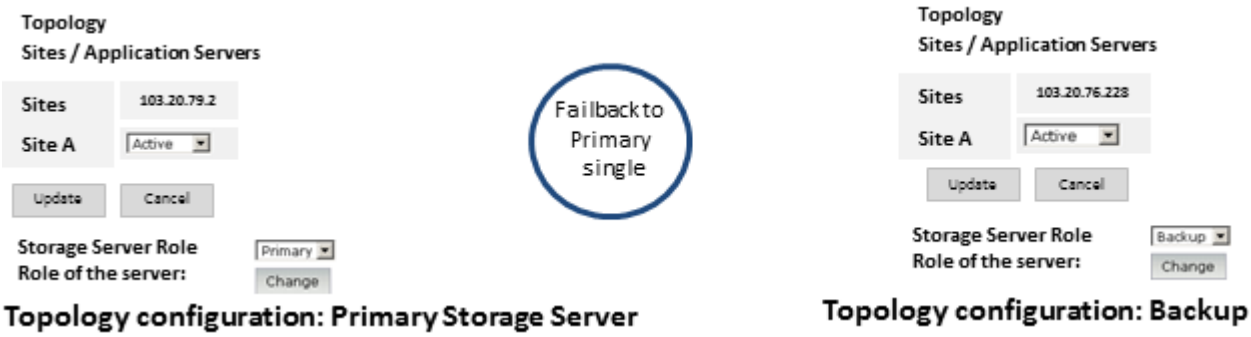
The following are examples of the topology page configuration.

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 Serv**

Multiserver configuration

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.

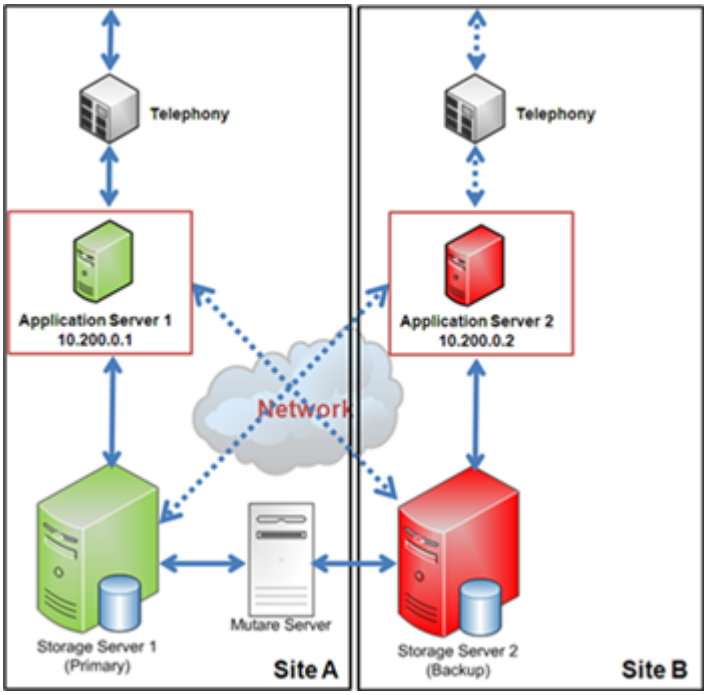
The following are examples of message store redundancy configuration with duplicated application servers.

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.

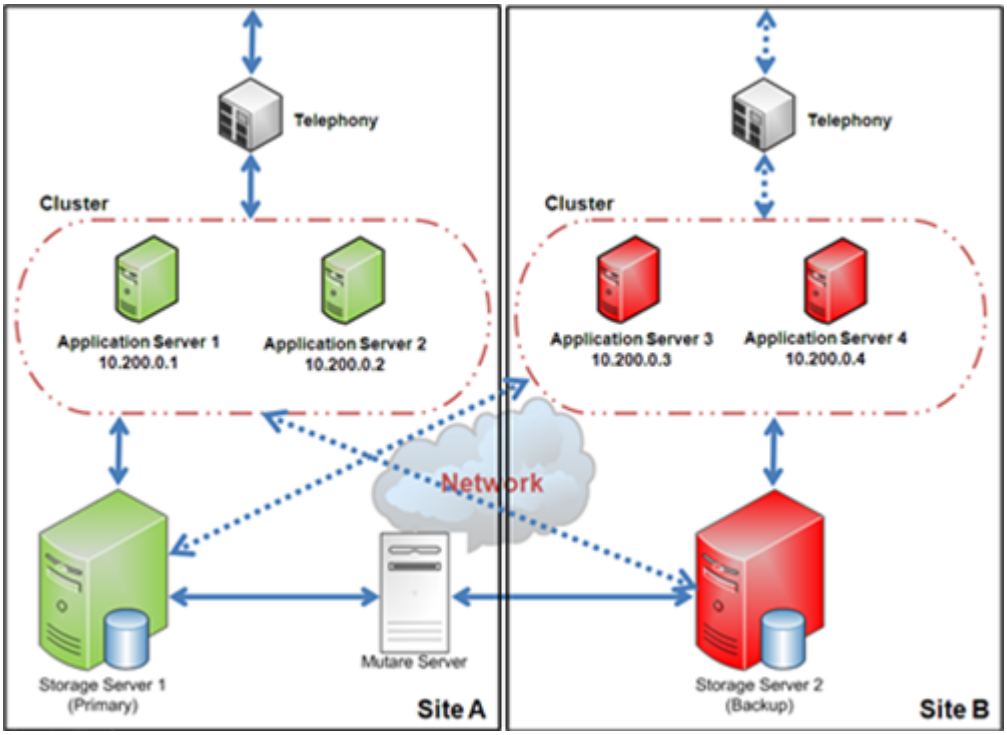
Failback service to the primary Messaging system.

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.

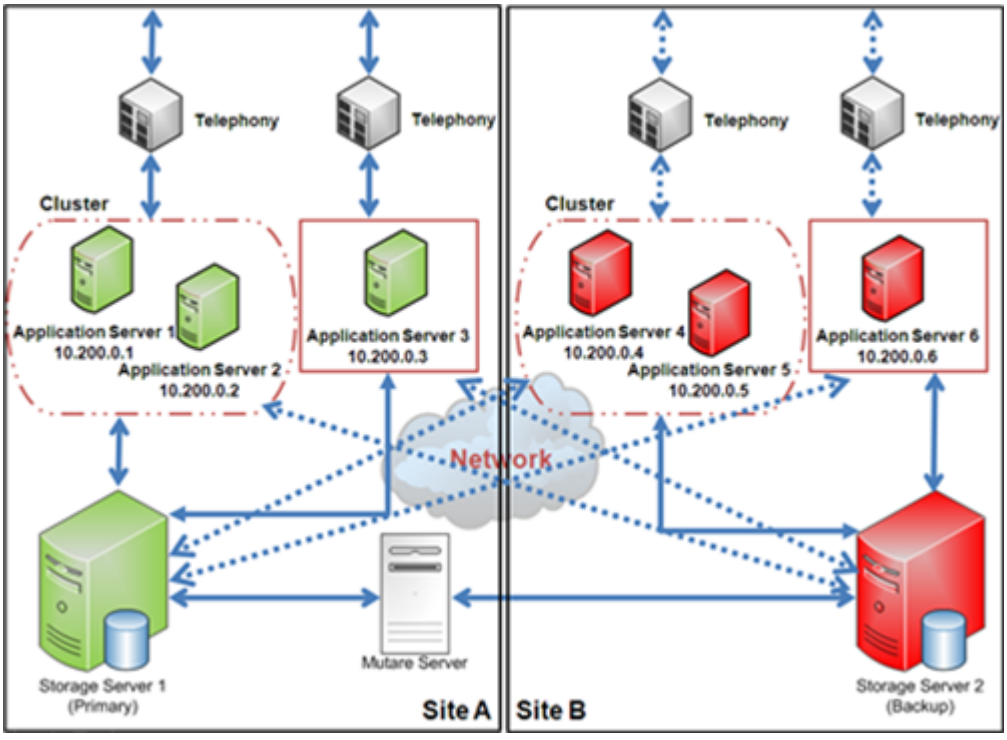
Failover service to the backup Messaging system.

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.

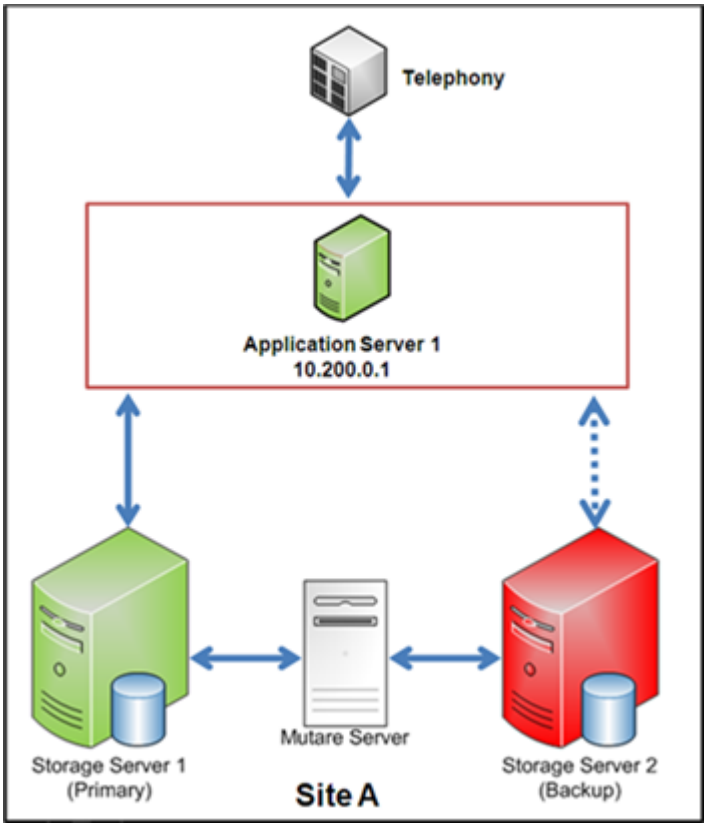
The following are examples of message store redundancy configuration with shared application servers.

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.

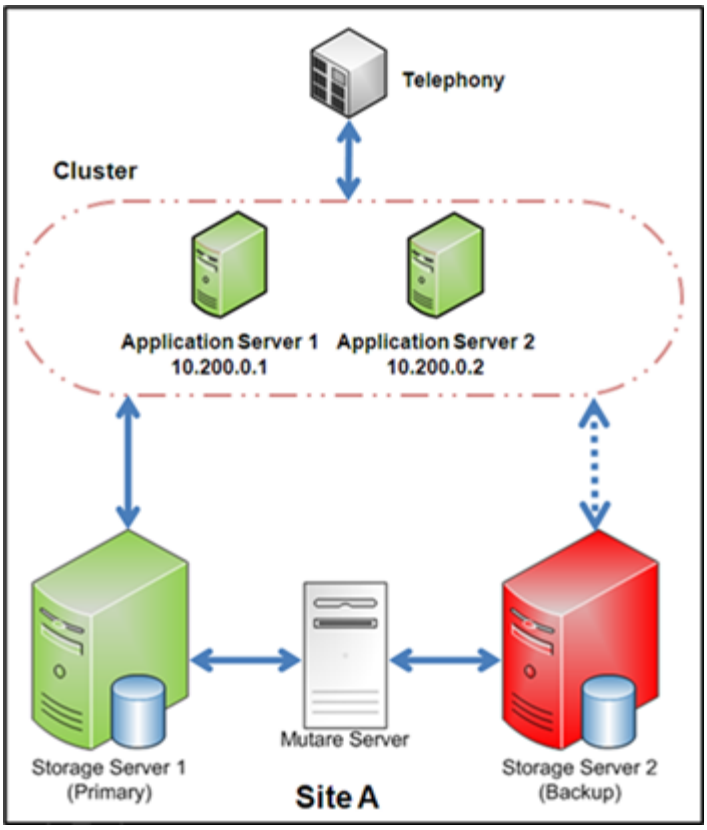
Failover service to the backup Messaging system.

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.

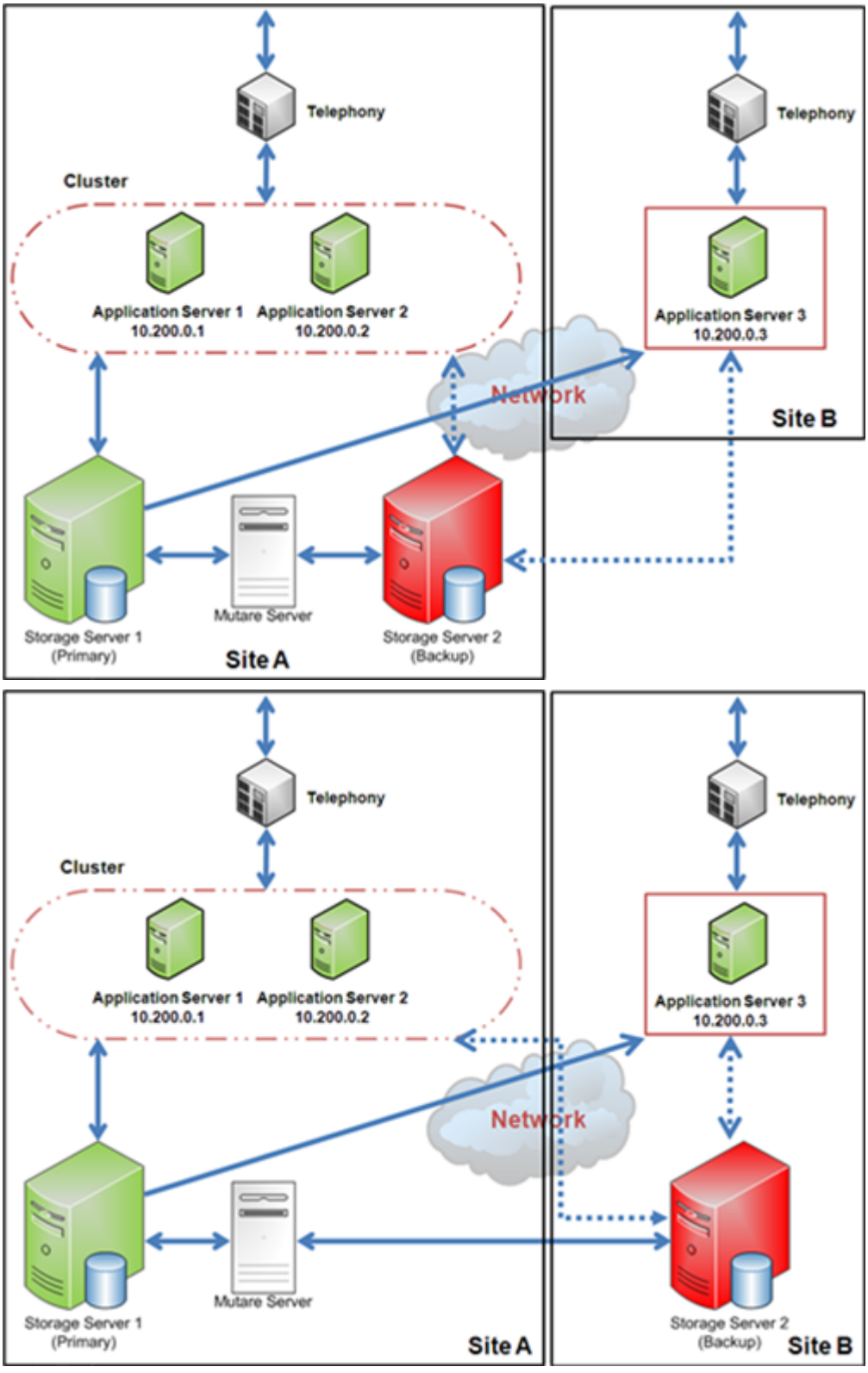
Failover service to the backup Messaging system.

(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.



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.

Planning and preconfigurations

Messaging Hardware and Software requirements

Hardware requirements

- Both the primary Messaging system and the backup Messaging system must run the HP ProLiant DL360p G9, HP ProLiant DL360p G8, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630.
- 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 with same Messaging software version.
- 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	2.4 GHz or faster processor; Quad-core preferred
System memory	4 GB RAM minimum (8 GB recommended)
Disk	100 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

Single 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 single server system.

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 • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*. .	• Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the primary Messaging system

	Server or System	Task	Required action
1	Primary system	Administer the primary server as a single-server system.	• Prepare the network. • Prepare the telephony server. • Set up the storage role. • Set up sites and topology.
2	Primary system	Add a new Message Mirror server as a trusted server. For more information, see Adding a trusted server on page 155.	• 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 the 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**.

Table continues…

	Server or System	Task	Required action
3	Primary system	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 393.	• 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.

Setting up networking with remote Messaging systems

	Server or System	Tasks	Required action
1	Primary system	Set up the primary system networking with remote Messaging systems. **Note:** Do this step only if you have a Remote Messaging system. For more information, see Setting up remote updates on page 210.	In the **Edit the Selected Networked Server** field, set the **Updates In** and **Updates Out** fields to **yes**.
2	Primary system	Add remote systems as a networked server. **Note:** Do this step only if you have a Remote Messaging system. For more information, see • Adding a network server on page 171. • Setting up remote updates on page 210.	• Add the remote systems. • Set the **Updates In** and **Updates Out** fields to **yes**.
3	Remote systems	Enable remote updates. **Note:** Do this step only if you have a Remote Messaging system. For more information, see Setting up remote updates on page 210	In the **Edit the Selected Networked Server** field, set the **Updates In** and **Updates Out** fields to **yes**.

Table continues…

	Server or System	Tasks	Required action
4	Remote systems	Add the primary system 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 171. • Setting up remote updates on page 210.	• Add the primary system. • Set the **Updates In** and **Updates Out** fields to **yes**.
5	Primary system	Request update for each remote system. For more information, see Running a remote update manually on page 211.	On the Request Remote Update webpage, click **remote system**, and click **Request Update**.
6	Primary system	Reload Global Address List Cache. For more information, see Loading lists on page 146.	To load Global Address List, click **Reload Caches** > **Reload**.
7	Remote system	Request update for the primary system. For more information, see Running a remote update manually on page 211.	On the Request Remote Update webpage, select **primary storage server**.
8	Remote system	Reload Global Address List Cache. For more information, see Loading lists on page 146.	To load Global Address List, click **Reload Caches** > **Reload**.

Preparing backup to be used for setting up backup system

	Server or System	Task	Required action
1	Messaging primary system	Back up the Messaging system data. For more information, see Backing up the system on page 284. Back up the Messaging data. For more information, see Backing up Messaging data on page 287.	On the Administration menu, click **Server Maintenance** > **Backup / Restore** click **Backup Now**. On the Backup Now webpage, in the Messaging area, select **Applications**, **Translations**, **Names**, and **Messages**. Click **Start Backup**.

Installing a license

Note:

- When you run Messaging in a VMware virtualized environment, install a separate WebLM VM or use a centralized WebLM. In this case, install a single license file that serves both the primary and the backup storage server.

You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

	Server or System	Task	Required action
1	Messaging primary system	Install Messaging license in WebLM server stand-alone, or embedded in Avaya System Manager for the primary system. For more information, see *License Management* in • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	—

Installing a backup system

	Server or System	Task	Required action
1	—	Install a backup system. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	• Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the backup system

	Server or System	Task	Required action
1	Messaging backup system	Restore the Messaging system data. For more information, see • Viewing restore history on page 297.	• Restore server, system, and security files. • Verify that restore status is `Success`.
2	Backup system	Stop Messaging. For more information, see Stopping Messaging on page 460	Stop Messaging.

Table continues…

	Server or System	Task	Required action
3	Backup system	Restore data that you backed up from the backup of primary system. For more information, see Performing a restore on page 294.	On the View/Restore Data webpage, click **Force Restore if server name mismatch or server migration**. Restore *Messaging Application, audix*.gz*.
4	Backup system	Start Messaging.	Start Messaging.
5	Backup system	Configure the storage server as a backup system. For more information, see Changing the storage server role on page 144.	In the **Storage Server Role** area, in the **Role of the Server** field, click **Backup**. **Note:** The backup system does not update MWI and LDAP on the application servers after you make storage server as the backup server.
6	Backup system	Stop Messaging. For more information, see Stopping Messaging on page 460.	Stop Messaging.
7	Backup system	Start Messaging.	Start Messaging.
8	Backup system	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 393.	• 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 networking with remote Messaging system

	Server or System	Task	Required action
1	Remote systems	Add the backup system 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 171. • Setting up remote updates on page 210.	• Add the backup server. • Set the **Updates In** field to **no** and **Updates Out** field to **yes**.
2	Backup system	Set up the backup system networking with remote Messaging systems. For more information, see Setting up remote updates on page 210.	• On the Manage Networked Servers webpage, select **remote system**, and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **no**.
3	Backup system	Request update for each remote system. For more information, see Running a remote update manually on page 211.	On the Request Remote Update webpage, click **remote system**, and click **Request Update**.
4	Backup system	Reload Global Address List Cache. For more information, see Loading lists on page 146	To load Global Address List, click **Reload Caches** > **Reload**.

Installing a license

Note:

- When you run Messaging in a VMware virtualized environment, install a separate WebLM VM or use a centralized WebLM. In this case, install a single license file that serves both the primary and the backup storage server.

You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

	Server or System	Task	Required action
1	Messaging backup system	Install Messaging license in WebLM server stand-alone, or embedded in Avaya System Manager for the backup system. For more information, see *License Management* in • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	—

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.	—

Setting up Telephony

	Server or System	Task	Required action
1	—	Add SIP trunk group to the primary system. For more information, see switch configuration notes.	—
2		Configure a route pattern.	—
3		Add SIP trunk group to the backup system.	—

Failover service to the backup system

Use the following checklist as a guide to switch service to the backup system.

Complete the tasks in the sequence that is listed in the checklist.

Changing DNS IP address

	Server or System	Task	Required action
1	—	Change the 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.	—

Setting up Telephony

	Server or System	Task	Required action
1	—	Add single SIP entity link for Avaya Aura® Messaging storage server. For more information, see Creating a single SIP entity of a storage server on page 100.	
2	—	Add two entries for Avaya Aura® Messaging storage server. For more information, see Creating local host name entries for storage server on page 102. For two local host name entries for storage server, use the same FQDN but different IP addresses. In the **Priority** field, ensure that backup failover store server has higher priority than the primary store server.	

Configuring the primary system as inactive

Note:

Perform this step only if the primary system is accessible.

	Server or System	Task	Required action
1	Primary system	Configure the primary system as a backup system. For more information, see Changing the storage server role on page 144.	In the **Storage Server Role** area, in the **Role of the Server** field, click **Backup**. **Note:** The system prevents LDAP updates to all application servers after you make storage server as the backup server. The MWI state is turned to its correct state.

Table continues…

	Server or System	Task	Required action
2	Primary system	Set up primary system networking with remote Messaging systems. Fore more information, see Setting up remote updates on page 210.	• On the Manage Networked Servers webpage, select **remote system** and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **no**.
3	Primary system	Stop Messaging. For more information, see Stopping Messaging on page 460.	—

Configuring the backup system as active

	Server or System	Task	Required action
1	Backup system	Configure the backup system as a primary system. For more information, see Changing the storage server role on page 144.	In the **Storage Server Role** area, in the **Role of the Server** field, click **Primary**. **Note:** The system updates the MWI and LDAP on the application servers after you make the storage server as the active server. The MWI state is turned to its correct state.
2	Backup system	Stop Messaging. For more information, see Stopping Messaging on page 460.	—
3	Backup system	Start Messaging. For more information, see Starting Messaging on page 460.	—
4	Backup system	Set up backup system networking with remote messaging systems. For more information, see Setting up remote updates on page 210.	• On the Manage Networked Servers webpage, select **remote system** and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **yes**.

Configuring remote Messaging systems

	Server or System	Task	Required action
1	Remote system	Delete primary system.	On the Manage Networked Servers webpage, select the **primary system** and click the **Delete the Selected Networked Server**.

Table continues…

	Server or System	Task	Required action
2	Remote system	Running Messaging database audit.	On the Messaging Database Audits (Storage) webpage, click **Start Network Data Audit (Machine Translations, Network Translations, Network Data)**.
3	Remote system	Enable remote updates.	On the Manage Networked Servers webpage, select the **backup system** and click the **Edit the Selected Networked Server**. Set the **Updates In** field to **yes**.
4	Remote system	Request update for the backup system. For more information, see Running a remote update manually on page 211.	On the Request Remote Update webpage, click **backup system**, and click **Request Update**.
5	Remote system	Reload Global Address List Cache. For more information, see Loading lists on page 146	To load Global Address List, click **Reload Caches** > **Reload**.

Failback service to the primary system

Use the following checklist as a guide to return service to the primary system.

Important:

Do the following tasks only during a planned downtime for system maintenance.

Complete the tasks in the sequence that is listed in the checklist.

Setting up Telephony

	Server or System	Task	Required action
1	—	Remove backup system trunk groups. For more information, see switch configuration notes.	—

Configuring the backup system as inactive

	Server or System	Task	Required action
1	Backup system	Configure the backup system. For more information, see Changing the storage server role on page 144.	In the **Storage Server Role** area, in the **Role of the Server** field, click **Backup**. **Note:** The system will not update the MWI and send LDAP updates to the application servers after you make storage server as the backup server.
2	Backup system	Set up backup system networking with remote Messaging systems. For more information, see Setting up remote updates on page 210.	• On the Manage Networked Servers webpage, select **remote system**, and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **no**.
3	Messaging backup system	Back up the Messaging system data. For more information, see Backing up the system on page 284.	On the Administration menu, click **Server Maintenance** > **Backup / Restore** click **Backup Now**.
4	Backup system	Back up the Messaging data. For more information, see Backing up Messaging data on page 287.	On the Backup Now webpage, in the Messaging area, select **Applications**, **Translations**, **Names**, and **Messages**. Click **Start Backup**.
5	Backup system	Start Messaging. For more information, see Starting Messaging on page 460.	—

Installing a primary system

	Server or System	Task	Required action
1	Primary system	Install a primary system. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*. .	• Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the primary system

	Server or System	Task	Required action
1	Messaging primary system	Restore the Messaging system data. For more information, see Viewing restore history on page 297.	• Restore server, system, and security files. • Verify that restore status is `Success`.
2	Primary system	Stop Messaging. For more information, see Stopping Messaging on page 460.	—
3	Primary system	Restore data that you backed up during step *4* from the backup of backup system. For more information, see Performing a restore on page 294	On the View/Restore Data webpage, click **Force Restore if server name mismatch or server migration**. Restore *Messaging Application, audix*.gz*.
4	Primary system	Start Messaging. For more information, see Starting Messaging on page 460.	—
5	Primary system	Configure the primary system.	In the **Storage Server Role** area, in the **Role of the Server** field, click **Primary**.
6	Primary system	Stop Messaging. For more information, see Stopping Messaging on page 460.	—
7	Primary system	Start Messaging. For more information, see Starting Messaging on page 460.	—

Configuring the primary system as active

	Server or System	Task	Required action
4	Primary system	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 393.	• 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.

Configuring remote Messaging systems

	Server or System	Task	Required action
1	Remote system	Delete backup system.	On the Manage Networked Servers webpage, select **primary system**, and click **Delete the Selected Networked Server**.
2	Remote system	Run Messaging database audit.	On the Messaging Database Audits (Storage) webpage, click **Start Network Data Audit (Machine Translations, Network Translations, Network Data)**.
3	Remote system	Add the primary system. **Note:** Do this step only if you have a Remote Messaging system. For more information, see Setting up remote updates on page 210.	• Set the **Updates In** and **Updates Out** fields to **yes**.
4	Remote system	Add the backup system.	• Set the **Updates In** to **no** and **Updates Out** field to **yes**.
5	Primary system	Enable remote updates. **Note:** Do this step only if you have a Remote Messaging system. For more information, see • Adding a network server on page 171. • Setting up remote updates on page 210.	• On the Manage Networked Servers webpage, select **remote system**, and click **Edit the Selected Networked Server**. Set the **Updates Out** field to **yes**.

Requesting updates for primary system

	Server or System	Task	Required action
1	Primary system	Request update for the remote system. For more information, see Running a remote update manually on page 211.	On the Request Remote Update webpage, click **remote system**, and click **Request Update**.
2	Primary system	Reload Global Address List Cache. For more information, see Loading lists on page 146.	To load Global Address List, click **Reload Caches** > **Reload**.

Table continues…

	Server or System	Task	Required action
3	Remote system	Request update for primary system. For more information, see Running a remote update manually on page 211.	On the Request Remote Update webpage, click **primary system**, and click **Request Update**.
4	Remote system	Reload Global Address List Cache. For more information, see Loading lists on page 146.	To load Global Address List, click **Reload Caches** > **Reload**.

Installing a license

Note:

- When you run Messaging in VMware virtualized environment, install a separate WebLM VM or use a centralized WebLM. In this case, install a single license file that serves both the primary and the backup storage server.

You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

	Server or System	Task	Required action
1	Messaging primary system	Install a license for the primary system. For more information, see *License Management* in • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	—

Enabling Mirror

	Server or System	Task	Required action
1	Message Mirror Admin interface	Enable Mirror. For more information, see the Mutare Software product documentation.	—

Setting up Telephony

	Server or System	Task	Required action
1.	__	Add primary system trunk groups. For more information, see switch configuration notes.	Disable call routing to the backup system, so that all calls route only to the primary system.

Multiserver configuration

Checklist for duplicated application server configuration

Initial setup of a new mirrored Messaging system

Use the following checklist to set up a new mirrored Messaging system with duplicated application servers.

Installing a primary Messaging system

No	Server or System	Task	Required action
1	—	Install a primary Messaging system. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*. .	• 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. For more information, see Integrating with the telephony server on page 134.	—
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 42.	In the **AxC IP address** field, enter the IP address of the primary storage server.

Table continues…

	Server or System	Task	Required action
3	Primary application server	Backup application files. For more information, see Backing up application files on page 287.	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 51. • Adding additional application servers on page 132.	• In the **Add Application Server** area, in the **IP address** field, enter the IP address of the application server you are joining to the cluster. • In the **Sites / Application Servers** area, in the **Default** field, click **Active**.
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 210.	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 171. • Setting up remote updates on page 210.	• Add the remote systems • Set the **Updates In** and **Updates Out** fields to **yes**.
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 171. • Setting up remote updates on page 210.	• Add the primary storage server. • Set the **Updates In** and **Updates Out** fields to **yes**.

Table continues…

	Server or System	Task	Required action
8	Primary storage server	Request update for each remote system. For more information, see Running a remote update manually on page 211.	On the Request Remote Update web page, click **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 146.	To load 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 211.	On the Request Remote Update web page, click **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 146.	To load 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 • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*. .	• 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.	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 application server. For more information, see Performing a restore on page 294.	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 134.	—
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 42.	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 51. • Adding additional application servers on page 132.	• In the **Add Application Server** area, 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** area, in the **Default** field, click **Inactive**.
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 144.	In the **Storage Server Role** area, in the **Role of the Server** field, verify that the storage server role is **Primary**. **Note:** The system applies LDAP updates to all application servers after you make storage server as the primary server. The MWI state is turned to its correct state.

Table continues…

	Server or System	Task	Required action
3	Primary storage server	Add a new Message Mirror server as a trusted server. For more information, see Adding a trusted server on page 155.	• 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 that 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 393.	• 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	Messaging primary storage server	Back up the Messaging system data.	On the Backup page, select the **Backup Now** option to start the backup operation immediately.
6	Primary storage server	Backup application files. For more information, see Backing up application files on page 287.	• 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 . • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	• Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the backup storage server

	Server or System	Task	Required action
1	Messaging backup storage server	Restore the Messaging system data. For more information, see Viewing restore history on page 297.	• Restore server, system, and security files. • 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 460. • Performing a restore on page 294. • Starting Messaging on page 460.	• 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 144.	• In the **Role of the Server** field, click **Backup**. • In the **Sites / Application Servers** area, click **Active** for each backup application server. • In the **Sites / Application Servers** area, click **Inactive** 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.

Table continues…

	Server or System	Task	Required action
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 393.	• 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 210.	Set the **Updates In** field to **yes** and **Updates Out** field to **no**.

Installing a license

Note:

- When you run Messaging in VMware virtualized environment, install a separate WebLM VM or use a centralized WebLM. In this case, install a single license file that serves both the primary and the backup storage server.

You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

	Server or System	Task	Required action
1	Messaging primary storage server	Install a license for the primary storage server. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	—

Table continues…

	Server or System	Task	Required action
2	Messaging backup storage server	Install a license for the backup storage server. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	—

Backing up storage server

	Server or System	Task	Required action
1	Backup storage server	Backup storage server. For more information, see Backing up the system on page 284.	—

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. For more information, see Changing the storage server role on page 144.	In the **Storage Server Role** area, in the **Role of the Server** field, click **Backup**. **Note:** The system prevents 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 144.	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 210.	• On the Manage Networked Servers webpage, 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 460.	—

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 144.	In the **Storage Server Role** area, in the **Role of the Server** field, click **Primary**. **Note:** The system updates the MWI and sends LDAP updates to all application servers after you make storage server as the active server. The MWI state is turned to its correct state.
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:** Do 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 393.	• 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 210.	• On the Manage Networked Servers webpage, 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 460.	—
5	Backup storage server	Start Messaging. For more information, see Starting Messaging on page 460.	—

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**. • In the **Reload Caches** area : - Click **Reload** next to the **User List** field to load User List. - Click **Reload** next to the **Global Address List** field to load Global Address List.

Setting up Telephony

	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 422.	• In the **Selection & Configuration** area, in the **Select the test(s) to run** field, click **Messages to Deliver**. • Click **Run Tests** periodically until **Voicemails to send** is 0.

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 171.	On the Manage Networked Server webpage, 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 211.	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 146.	To load 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 211.	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 146.	To load Global Address List, click **Reload Caches** > **Reload**.

Restarting Messaging Web Access

	Server or system	Task	Required actions
1	Single server or application server	Restart Messaging Web Access. For more information, see Restarting Messaging Web Access on page 458.	To restart Messaging Web Access, click **Restart Messaging Web Access** > **Restart**.

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:

Do 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	Messaging backup storage server	Back up the Messaging system data.	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 287.	• 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 144.	In the **Storage Server Role** area, in the **Role of the Server** field, click **Backup**.

Table continues…

	Server or System	Task	Required action
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 393.	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 210.	• On the Manage Networked Servers webpage, 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 460.	—
7	Backup storage server	Start Messaging. For more information, see Starting Messaging on page 460.	—

Installing a primary storage server

	Server or System	Task	Required action
1	Primary storage server	Install a primary storage server. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*. .	• Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the primary storage server

	Server or System	Task	Required action
1	Messaging primary storage server	Restore the Messaging system data. For more information, see Viewing restore history on page 297	• Restore server, system, and security files. • Verify that restore status is `Success`.
2	Primary storage server	Restore data that you backed up from the backup storage server. For more information, see • Stopping Messaging on page 460. • Performing a restore on page 294. • Starting Messaging on page 460.	• 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** area, in the **Default** field, click **Active** for each primary application server. • In the **Sites / Application Servers** area, in the **Default** field, click **Inactive** 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 393.	• 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 Administering the server role and AxC IP address on page 42.	In the **AxC IP address** field, enter the IP address of the primary storage server.

Table continues…

	Server or System	Task	Required action
2	Primary application server	Reload User List and Global Address List.	• On the **Administration** menu, click **Messaging** > **Advanced (Application)** > **System Operations**. • In the **Reload Caches** area : - Click **Reload** next to the **User List** field to load User List. - Click **Reload** next to the **Global Address List** field to load 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 171.	On the Manage Networked Server webpage, 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 211.	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 146.	To load 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 211.	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 146.	To load Global Address List, click **Reload Caches** > **Reload**.

Installing a license

Note:

- When you run Messaging in VMware virtualized environment, install a separate WebLM VM or use a centralized WebLM. In this case, install a single license file that serves both the primary and the backup storage server.

You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

	Server or System	Task	Required action
1	Messaging primary storage server	Install a license for the primary storage server. • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	—

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.	—

Restarting Messaging Web Access

	Server or system	Task	Required actions
1	Single server or application server	Restart Messaging Web Access. For more information, see Restarting Messaging Web Access on page 458.	To restart Messaging Web Access, click **Restart Messaging Web Access** > **Restart**.

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. • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	• 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 134.	—
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 42.	In the **AxC IP address** field, enter the IP address of the primary storage server.

Table continues…

	Server or System	Task	Required action
3	Primary storage server	Add application servers. For more information, see • Adding the first application server on page 51. • Adding additional application servers on page 132.	• In the **Add Application Server** area, in the **IP address** field, enter the IP address of the application server you are joining to the cluster. • In the **Sites / Application Servers** area, in the **Default** field, click **Active**.
4	Primary storage server	Set up the storage server networking with remote Messaging systems. **Note:** Do this step only if you have a Remote Messaging system. For more information, see Setting up remote updates on page 210.	Set the **Updates In** and **Updates Out** fields to **yes**.
5	Primary storage server	Add remote systems as a networked server. **Note:** Do this step only if you have a Remote Messaging system. For more information, see • Adding a network server on page 171. • Setting up remote updates on page 210.	• 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 171. • Setting up remote updates on page 210.	• 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 211.	On the Request Remote Update webpage, click **remote system** from the drop-down list.

Table continues…

	Server or System	Task	Required action
8	Application server	For each application server, reload Global Address List Cache. For more information, see Loading lists on page 146.	To load Global Address List, click **Reload Caches** > **Reload**.
9	Remote system	Request update for the primary storage server. For more information, see Running a remote update manually on page 211.	On the Request Remote Update webpage, 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 146.	To load 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 144.	In the **Storage Server Role** area, in the **Role of the Server** field, 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. The MWI state is turned to its correct state.

Table continues…

	Server or System	Task	Required action
2	Primary storage server	Add a new Message Mirror server as a trusted server. For more information, see Adding a trusted server on page 155.	• 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**.
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 393.	• 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	Messaging primary storage server	Back up the Messaging system data.	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 287.	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 • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*. .	• Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the backup storage server

	Server or System	Task	Required action
1	Messaging backup storage server	Restore the Messaging system data. For more information, see Viewing restore history on page 297.	• Restore server, system, and security files. • 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 460. • Performing a restore on page 294. • Starting Messaging on page 460.	• 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 144.	• In the **Storage Server Role** in the **Role of the Server** field, click **Backup**. • In the **Sites / Application Servers** area, click **Shared** from the drop-down list for each 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.

Table continues…

	Server or System	Task	Required action
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 393.	• 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 the storage server networking with remote Messaging systems. For more information, see Setting up remote updates on page 210.	Set the **Updates In** field to **yes** and **Updates Out** field to **no**.

Installing a license

Note:

- When you run Messaging in VMware virtualized environment, install a separate WebLM VM or use a centralized WebLM. In this case, install a single license file that serves both the primary and the backup storage server.

You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

	Server or System	Task	Required action
1	Messaging primary storage server	Install a license for the primary storage server. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*. .	—

Table continues…

	Server or System	Task	Required action
2	Messaging backup storage server	Install a license for the backup storage server. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*. .	—

Backing up storage server

	Server or System	Task	Required action
1	Backup storage server	Backup storage server. For more information, see Backing up the system on page 284.	—

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 the 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:

Do 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 144.	• In the **Storage Server Role** area, in the **Role of the Server** field, click **Backup**. • In the **Sites / Application Servers** area, click **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 144.	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 210.	• On the Manage Networked Servers webpage, 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 460.	—

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 User List and Global Address List. For more information, see Administering the server role and AxC IP address on page 42.	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 144.	• In the **Sites / Application Servers** area, in the **Default** field, click **Active** from the drop-down list next to the site. • In the **Storage Server Role** area, in the **Role of the Server** field, click **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 393.	• 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 210.	• On the Manage Networked Servers webpage, select **remote system** and click **Edit the Selected Networked Server**. • Set the **Updates Out** field to **yes**.

Table continues…

	Server or System	Task	Required action
4	Backup storage server	Stop Messaging. For more information, see Stopping Messaging on page 460.	—
5	Backup storage server	Start Messaging. For more information, see Starting Messaging on page 460.	—

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**. • In the **Application Distributed Cache (ADCS) Maintenance** field, 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**. • In the **Reload Caches** area, do the following: - In the **User List** field, click **Reload**. - In the **Global Address List** field, click **Reload**.

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 171.	On the Manage Networked Server webpage, change the value for the following fields: • Hostname • IP address • Password

Table continues…

	Server or System	Task	Required action
2	Remote system	Request update for the backup storage server. For more information, see Running a remote update manually on page 211.	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 146.	To load 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 211.	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 146.	To load Global Address List, click **Reload Caches** > **Reload**.

Restarting Messaging Web Access

	Server or system	Task	Required actions
1	Single server or application server	Restart Messaging Web Access. For more information, see Restarting Messaging Web Access on page 458.	To restart Messaging Web Access, click **Restart Messaging Web Access** > **Restart**.

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:

Do 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	Messaging backup storage server	Back up the Messaging system data.	On the Backup page, to start the backup operation immediately, select the **Backup Now** option.
2	Backup storage server	Backup application files. For more information, see Backing up application files on page 287.	• 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 144.	• In the **Storage Server Role** area, in the **Role of the Server** field, click **Backup**. **Note:** The system prevents LDAP updates to all application servers after you make storage server as the backup server. The MWI state is turned to its correct state. • In the **Sites / Application Servers** area, click **Shared** from the drop-down list for each application server.

Table continues…

	Server or System	Task	Required action
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:** Do 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 393.	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 210.	• On the Manage Networked Servers webpage, 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 460.	—
7	Backup storage server	Start Messaging. For more information, see Starting Messaging on page 460.	—

Installing a primary storage server

	Server or System	Task	Required action
1	Primary storage server	Install a primary storage server. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	• Install Messaging. • Install Communication Manager and Messaging patches.

Configuring the primary storage server

	Server or System	Task	Required action
1	Messaging primary storage server	Restore the Messaging system data. For more information, see Viewing restore history on page 297.	• Restore server, system, and security files. • 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 460. • Performing a restore on page 294. • Starting Messaging on page 460.	• 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 393.	• 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	Primary storage server	Start Messaging. For more information, see Starting Messaging on page 460.	—

Changing the AxC address

	Server or System	Task	Required action
1	Primary application server	Change the AxC address. For more information, see Administering the server role and AxC IP address on page 42.	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**. • In the **Reload Caches** area, do the following: - In the **User List** field, click **Reload**. - In the **Global Address List** field, click **Reload**.

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 171.	On the Manage Networked Server webpage, 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 211.	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 146.	To load 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 211.	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 146.	To load Global Address List, click **Reload Caches** > **Reload**.

Installing a license

Note:

- When you run Messaging in VMware virtualized environment, install a separate WebLM VM or use a centralized WebLM. In this case, install a single license file that serves both the primary and the backup storage server.

You can use the Avaya Product Licensing and Delivery System (PLDS) to generate and download license files.

	Server or System	Task	Required action
1	Messaging primary storage server	Install a license for the primary storage server. For more information, see. • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	—

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.	—

Restarting Messaging Web Access

	Server or system	Task	Required actions
1	Single server or application server	Restart Messaging Web Access. For more information, see Restarting Messaging Web Access on page 458.	To restart Messaging Web Access, click **Restart Messaging Web Access** > **Restart**.

Checklist for upgrading Messaging system

Set up a mirrored Messaging system. See Initial setup of a new mirrored Messaging system on page 516

No.	Task	References		Notes
		Duplicated	Shared	
1.	Failover services to the backup Messaging system 1. Change the DNS IP address 2. Disable Mirror 3. Configure the primary storage server as inactive 4. Configure the primary storage server as backup server 5. Verify that the storage server is configured as a backup server 6. Set up the storage server networking with remote Messaging systems 7. Stop Messaging 8. Configure the backup storage server as active 9. Configure the backup storage server as a primary server 10. Configure the mail options 11. Set up the storage server networking with remote Messaging systems 12. Stop Messaging 13. Start Messaging 14. Reload User List and Global Address List	See Failover service to the backup Messaging system on page 523.	See Failover service to the backup Messaging system on page 539.	-

Table continues…

No.	Task	References		Notes
		Duplicated	Shared	
	15. Remove all application server trunk groups 16. Add all backup application server trunk groups 17. Run diagnostic test to ensure that all offline messages are delivered to the new primary storage server 18. Configure remote Messaging systems 19. Configure the primary storage server as a networked server 20. Request update for the backup storage Server 21. Reload Global Address List Cache for each application server 22. Request updates for the backup storage server 23. Request update for the remote system 24. Reload Global Address List Cache for each application server			
2.	Upgrade the Messaging system	-		-

Table continues…

No.	Task	References		Notes
		Duplicated	Shared	
3.	Failback services to the primary Messaging system 1. Disable routing of calls 2. Change DNS IP address 3. Configure the backup storage server as inactive 4. Backup the system files 5. Back up application files 6. Configure the storage server as backup server 7. Configure the mail options 8. Set up storage server networking with remote Messaging systems 9. Stop Messaging 10. Start Messaging 11. Install a primary storage server 12. Configure the primary storage server 13. Restore backed up data 14. Configure the primary storage server as active 15. Configure the mail options 16. Change the AxC address	See Failback service to the primary Messaging system on page 527.	See Failback service to the primary Messaging system on page 543.	-

Table continues…

No.	Task	References		Notes
		Duplicated	Shared	
	17. Reload User List and Global Address List 18. Configure remote Messaging systems 19. Configure the storage server from backup to primary 20. Request update for the primary storage server 21. Reload Global Address List Cache for each application server 22. Request updates for primary storage server 23. Request update for the remote system 24. Reload Global Address List Cache for each application server 25. Install a license for the primary storage server 26. Enable Mirror 27. Enable call routing to all primary application servers 28. Restart Messaging Web Access, if applicable.			

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 189.	
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 348.	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 422	
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 348.	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 422	

Table continues…

Tasks	Server	Steps	Result / Validate
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. 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.
(Optional) Perform configuration testing.		You can perform the following testing on primary and backup systems. • Configuration of remote users • Call routing	

Chapter 21: 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.
4. To reload User List, click **Reload**.
5. To reload 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.

Proposed solution

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **Messaging DB Audits (Storage)**.
2. Click the following links to perform the audit:
   - **Start Mailbox Audit**: Sends the correct MWI updates for the user on the system.
   - **Start Subscriber Data Audit**: Fixes the errors and sends the correct MWI state for the user on the system.

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.

Proposed solution

Check the connection between the Exchange Server and the Messaging server.

Procedure

1. On Exchange Server, navigate to `\WINDOWS\system32\LogFiles\W3SVC1`, and check if Exchange Server receives the email from Messaging.
2. To determine whether Exchange Server is working, check the CPU use and memory of Exchange Server.

Fax troubleshooting

The following common errors are the result of incorrect configuration:

Condition	Result
You configured CoS for fax support, but the fax email is unavailable.	Messaging rejects fax during the transmission.
You configured CoS for fax support, but the fax email is unavailable and AxC is offline.	Messaging sends the fax to the postmaster account.
You configured an incorrect email address.	Messaging sends DSN to the postmaster account.

Validate whether you implemented fax correctly.

Related links

Fax administration checklist on page 112

Outbound fax

To enable outbound fax for users, you must enable the **Fax support** option in the Class of Services (COS) page for one of the following:

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

User cannot send a fax to a destination number

Condition

The user cannot send a fax to the destination number. The destination numbers can be:

- On premise
- Local
- Long distance
- International

Cause

User does not have the appropriate dial-out privileges to call the destination number.

Solution

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. In the **Class of Service** field, click the type of CoS to which the user belongs.
3. In the **Dial-out privilege** field, click the appropriate options.

   Do not click **None**, else the user cannot send the fax to the destination number.
4. Click **Save**.

User cannot add the fax printer

Condition

The user cannot add the fax printer to the computer.

Cause

Fax support for the user is not enabled in CoS.

Solution

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. In the **Fax support** field, do the following:
   - Click **Receive and forward to email**.
   - Click **Detect and transfer to fax server**.
3. Click **Save**.

Application server fails to send the fax to the target fax machine

Condition

The user can print the fax but cannot send the fax to the target fax machine.

Solution

1. Log in to Messaging SMI from the application server, and on the **Administration** menu, click **Messaging** > **Diagnostics** > **Diagnostics (Application)**.
2. In the **Selection & Configuration** section, in the **Select the test(s) to run** field, click **Fax Outcall**.

   The system displays the Configuration of Fax Outcall Test page.
3. In the **Fax number** field, type the fax number.
4. Clear the **Use default telephony parameters** check box.

   The Configuration of Fax Outcall Test page displays the following fields:
   - **Telephony profile name**
   - **Caller ID name**
   - **Caller ID number**
   - **P-Asserted Identity name**
   - **P-Asserted Identity number**
   - **Fax size**
5. Type the information in the fields.

   If the system has multiple sites configured, ensure that the telephony profile value matches the value of the site that the user belongs to.

6. Click **Run Tests**.
7. Verify if a specific application server is sending the fax successfully to a specified number.

Messaging displays the Too many invalid login attempts message

Messaging displays the `Too many invalid login attempts` to a user whose mailbox is not locked.

Troubleshooting steps

Procedure

1. Check that the mailbox of the user is not locked. If the mailbox of the user is locked:
   a. On the **Administration** menu, click **Messaging** > **Reports (Storage)** > **Users**.
   b. Use the built-in filters to find the mailbox that you want to check and click the **Mailbox** number.
   c. On the User Management > Properties webpage, select the **Unlocked** option.

      When the mailbox is unlocked by the administrator, the **Locked Out due to excessive Invalid Login Attempts** option is disabled in the system.

      By selecting the **Unlocked** option, the user can use the correct login credentials to log in to the voice mailbox at the next logon. Messaging automatically locks the mailbox when the user fails to enter proper login credentials after a certain number of consecutive failed attempts.

      Using the **Consecutive Invalid Attempts** field on the System Administration webpage, you can set the number of consecutive failed attempts for the system.
2. Click **Save**.
3. If the user still receives the `Too many invalid login attempts` message, check whether:
   a. The user is an Exchange user.
   b. The Exchange mailbox of the user is deleted.

MWI notifications and NotifyMe calls fail

Messaging delivers MWI notifications and makes NotifyMe calls through the storage server.

Proposed solution

Procedure

1. On the **Administration** menu, click **Messaging** > **Utilities** > **Messaging DB Audits (Storage)**.
2. Click the following links to perform the audit:
   - **Start Mailbox Audit**: Sends the correct MWI updates for the user on the system.
   - **Start Subscriber Data Audit**: Fixes the errors and sends the correct MWI state for the user on the system.

   After the issue is resolved, MWI is turned to its correct state after restarting Messaging on the storage server.

Related links

Running application server diagnostics on page 422
Stopping Messaging on page 460
Starting Messaging on page 460
Ping on page 429
Traceroute on page 431
Netstat on page 434

Notify Me feature for SMS does not function properly

Condition

When a large number of messages originate from the same Messaging IP address, the Notify Me feature for SMS stops functioning.

Cause

Mobile carriers might disable the service. This is because mobile carriers might consider the large number of messages from the same IP address as spam.

Solution

Contact the mobile operator and ensure that:

- The mobile operator has not blocked SMS from the Messaging IP address or FQDN (Fully Qualified Domain Name).
- The mobile operator can resolve and “white-list” the Messaging IP address or FQDN.

MWI displays an incorrect status of user’s voice messages

Condition

In some cases, the MWI light might not indicate a correct status of user’s voice messages. For example, the MWI light turned off when the user has unread voice messages.

Solution

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. In the Edit User/Info Mailbox section, in the **Identifier** field, type the user identifier and then click **Edit**.

   Messaging displays the **User Management** > **Properties** page.
3. In the **Advanced Tasks** > **Reset the message waiting indicator for extension** area, click **Reset**.
4. Ensure that Messaging does not display any error messages.
5. If Messaging displays the `Message waiting light cannot be reset` error, contact the Avaya support.

Messaging certificate fails to load or displays the Could not get local user message

Proposed solution

Procedure

1. Verify that the Messaging FQDN is correct.
2. Verify that the file name of the certificate has the .pem or the .crt extension.
3. If the CA is VeriSign, install the CA Root certificate and the intermediate certificate.

Related links

Generating a certificate signing request on page 402

Default value of voice mail message length changes

Condition

When you upgrade Messaging to Release 6.3.1 or later, the value of maximum voice mail message length changes.

Cause

Before Release 6.3.1, the maximum voice message length on the Systems Parameters (Application) webpage of the Messaging System Management Interface controlled the maximum voice mail message length.

After upgrading to 6.3.1 or later, the Class of Service (Storage) webpage supersedes the maximum voice message length.

Solution

1. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. In the **Message Storage** section, change the value of **Maximum voice message length**.
3. Click **Save**.

Text-To-Speech does not play prompts

Condition

VXIBrowser does not play text for user names and voice prompts from vxml pages.

Cause

After entering the FQDN of the server, Messaging system is not restarted.

Solution

1. Log on to the Messaging System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)** > **Server Configuration** > **Network Configuration**.
3. Click **Continue** at the warning.
4. On the **Network configuration** page, in the **DNS Domain** field, verify that you have entered the FQDN of the server.
5. Click **Save**.
6. Restart Messaging.

Extension entered does not match the length specified in site

Condition

When you add a new user or new Info Mailbox or edit the details for an existing user and change the **Extension number**, the system displays the following error message: `Extension entered doesn't match the length specified in site.`

Cause

The Messaging storage server verifies that the primary **Extension length** is the same or longer than the **Site identifier length** (for E.164 formats) + '**Short extension length**' specified on the Sites page.

Solution

Ensure that the **Extension number** that you enter complies with the following requirements:

- If you add or edit a user which belongs to the site with **Short Extension** style and **Short extension length** = n, then you must enter n or more digits for **Extension number**.
- If you add a user which belongs to the site with E.164 formats and **Short extension length** = n, then you must enter n or more digits for **Extension number**.
- If you edit a user which belongs to the site with E.164 formats and **Short extension length** = n, then you must ensure that the full **Extension number length** is the same or longer than the **Site identifier length** + '**Short extension length**' specified on the Sites page.
- If you add a new user or new Info Mailbox and the primary **Extension** was not explicitly entered, it will be set using the **Mailbox number**. In this case Messaging storage server verifies that the **Mailbox number length** is the same or more then **Site identifier length** (for E.164 formats) + '**Short extension length**' specified on the Sites page.

The mailbox number cannot be saved since it does not match the mailbox length (N digits)

Condition

When you add a new user or new Info Mailbox or edit the details for an existing user and change the **Mailbox number**, the system displays the following error message: `The mailbox number xxxxxxxxxxx cannot be saved since it does not match the mailbox length (N digits). Please verify the site definition and/or the mailbox length. LDAP Error 1512.`

Cause

The Messaging storage server verifies that the **Mailbox length** is exactly the same as the **Mailbox Number Length** specified on the Networked Servers page.

Solution

Ensure that the **Mailbox Number Length** matches the following requirements under given conditions:

- Your Messaging system manages multiple sites, each of which requires the different number of digits for their telephone extension and mailbox combination: In this case, ensure that the **Mailbox Number Length** is set as **Variable** on the **Networked Servers** page.
- Your Messaging system manages multiple sites, each of which requires the same number of digits for their telephone extension and mailbox combination: In this case, if you add or edit a new user or new Info Mailbox and change the **Mailbox number**, ensure that your entered **Mailbox number length** corresponds to the **Mailbox Number Length** specified on the Networked Servers page.

Certain phone numbers are not dialed or not conserved

Condition

User has insufficient dialling privileges to call.

Cause

The dial out rules fields described in SMI Site External (Public Network) Dial Plan section are used to generate dial out string to send to the PBX for various subscriber activities where a phone number is specified. For example, ReachMe, NotifyMe, Call Sender, Play on Phone, Personal attendant or assistant. As each subscriber is associated to a site, Messaging applies the corresponding site dial plan parameters to categorize the phone number type (internal, local, long distance, international) and generate the appropriate dial out string. Using the phone number type, Messaging evaluates whether the associated user has the required dial-out privilege in their COS.

Solution

Go to **Administration** menu, click **Messaging** > **Server Settings (Application)** > **Dial Rules** and do the following:

a. To verify how site dial-out settings handle one or another phone number, in Dial Plan Handling section, in the **Dial plan handling style**, click **Site definition based** and click **Test**.

b. To verify whether the Dial-Out Rules script handles these numbers correctly, in Dial Plan Handling section, in the **Dial plan handling testing**, click **Test**. On the Dial Plan Handling Test page, enter the **Site ID** value and define the phone numbers one per line.

   In the Dial-Out Test Results section, you can see the Call Type. The call type could be internal, local, long distance, international, or invalid.

c. To verify if the associated user has the required dial-out privileges in CoS, go to **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**. If the number is internal, then in the **Dial-out privilege** field, click **On Premise**. If the number is long distance, then click **Long Distance**, or **Long distance** or **International**.

Chapter 22: Resources

Documentation

You can download the documents you need from the Avaya Support website at https://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 links

Overview on page 566
Deployment, upgrade, and migration on page 569

Overview

Title	Description	Audience
Avaya Aura® Messaging Overview and Specification	Describes tested product characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales and deployment engineers, solution architects, and support personnel.
Avaya Aura® Messaging Single Server Reference Configuration	Describes the design, capacities, interoperability, and limitations of single-server configurations.	Sales and deployment engineers, solution architects, and support personnel.
Avaya Aura® Messaging Multiserver Single Location Reference Configuration	Describes the design, capacities, interoperability, and limitations of multi-server single location configurations.	Sales and deployment engineers, solution architects, and support personnel.
Avaya Aura® Messaging Multiserver Dual Location Reference Configuration	Describes the design, capacities, interoperability, and limitations of multi-server dual location configurations.	Sales and deployment engineers, solution architects, and support personnel.

Table continues…

Title	Description	Audience
Avaya Aura® Messaging VMware® in the Virtualized Environment Reference Configuration	Describes the design, capacities, interoperability, and limitations of VMware® in the virtualized environment configurations.	Sales and deployment engineers, solution architects, and support personnel.

Related links

Documentation on page 566

Security

Title	Description	Audience
Avaya Aura® Messaging Security Design	Discusses security issues to consider when designing a corporate security strategy. Topics include network security, toll fraud, and recommendations for maintaining a secure system.	Solution architects, deployment engineers, and administrators

User functions

Title	Description	Audience
Using Avaya Aura® Messaging	Explains how to set up and use User Preferences and the Messaging toolbar in your email client. The content is available in two formats: HTML and PDF.	Users
Using Avaya Aura® Messaging Job Aid	Includes the most common user tasks. This job aid is a subset of the user guide.	Users and support personnel
Avaya Aura® Messaging Quick Reference (Aria)	Describes how to use the Aria telephone user interface.	Users
Avaya Aura® Messaging Quick Reference (Audix®)	Describes how to use the Audix® telephone user interface.	Users
Avaya Aura® Messaging Quick Reference (CallPilot®)	Describes how to use the CallPilot telephone user interface.	Users

Hardware

New installations

Title	Description	Audience
Installing the Dell™ PowerEdge™ R620 server	Describes the components, specifications, and configurations for this server.	Deployment engineers and support personnel.
Installing the Dell™ PowerEdge™ R630 Server	Describes the components, specifications, and configurations for this server.	Deployment engineers and support personnel.
Installing the HP ProLiant DL360p G8 server	Describes the components, specifications, and configurations for this server.	Deployment engineers and support personnel.
Installing the HP ProLiant DL360 G9 Server	Describes the components, specifications, and configurations for this server.	Deployment engineers and support personnel.

Maintenance

Title	Description	Audience
Maintaining and Troubleshooting the Dell™ PowerEdge™ R620 server	Describes how to add, replace, and repair hardware components for this server.	Deployment engineers and support personnel.
Maintaining and Troubleshooting the Dell™ PowerEdge™ R630 Server	Describes how to add, replace, and repair hardware components for this server.	Deployment engineers and support personnel.
Maintaining and Troubleshooting the HP ProLiant DL360p G8 server	Describes how to add, replace, and repair hardware components for this server.	Deployment engineers and support personnel.
Maintaining and Troubleshooting the HP ProLiant DL360 G9 Server	Describes how to add, replace, and repair hardware components for this server.	Deployment engineers and support personnel.

Deployment, upgrade, and migration

Title	Description	Audience
Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment	Describes procedures for deploying the Avaya Aura® Messaging virtual application in the Avaya Aura® Virtualized Environment. The procedures relate to installation, configuration, initial administration, troubleshooting, and basic maintenance of the application.	Deployment engineers, solution architects, and support personnel.
Deploying Avaya Aura® Messaging using Solution Deployment Manager	Describes procedures for deploying the Avaya Aura® Messaging virtual application in the Appliance Virtualization Platform. The procedures relate to installation, configuration, initial administration, troubleshooting, and basic maintenance of the application.	Deployment engineers, solution architects, and support personnel.

Related links

Documentation on page 566

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 might differ from the titles shown.

Course code	Course title
4311W	Selling Unified Communication Messaging — Overview
5U00140V	Avaya Aura® Messaging Implementation, Administration, and Support Virtual Instructor Led
5U00140I	Avaya Aura® Messaging Implementation, Administration, and Support Instructor Led
ATI01674VEN	Avaya Aura® Messaging — Caller Applications

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://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.

Related links

Using the Avaya InSite Knowledge Base on page 571

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 570

Warranty

Avaya provides a 3-month limited warranty on Messaging. Detailed terms and conditions are contained in the sales agreement or other applicable documentation that 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*.

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, your server A has 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 • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	—	• Install Messaging. • Install Communication Manager and Messaging patches.
1b	Install application server C. For more information, see • *Deploying Avaya Aura® Messaging using Solution Deployment Manager*. • *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*.	—	• Install Messaging. • Install Communication Manager and Messaging patches.

Table continues…

No.	Task	Server or system	Required action
2	For each application server, change the AxC address.	—	—
2a	On application server B, change the AxC address. For more information, see Administering the server role and AxC IP address on page 42.	Server B	In the **AxC IP address** field, enter the IP address of server A.
2b	On application server C, change the AxC address. For more information, see Administering the server role and AxC IP address on page 42.	Server C	In the **AxC IP address** field, enter the IP address of server A.
3	Add application servers.	—	—
3a	Add server B as an application server. For more information, see Adding the first application server on page 51.	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.
3b	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.
4	For each application server, update the cluster configuration.	—	—
4a	Define the application server C as a member of the cluster. For more information, see Configuring a cluster on page 110.	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.
4b	Define the application server B as a member of the cluster. For more information, see Configuring a cluster on page 110.	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.

Table continues…

No.	Task	Server or system	Required action
5	Assign sites to the new Application Server(s) / Roles and Update Topology. For more information, see Adding the first application server on page 51.	Server B	In the **Add Application Server** area: • From the **Add the server with** heading, select **Same site configuration as an existing application server**. • In the **IP Address** drop-down menu, click the IP address of server A.
6	Busy out the application server. For more information, see Busying out voice channels on page 397.	Server A	—
7	Remove application server A.	Server A	• On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **Topology**. • In the **Remove Application Server** area, select the IP address of server A. • Click **Remove**.
8	Change Switch Integration. For more information, see Integrating with the telephony server on page 134.	Server A	In the **Switch Integration Type** drop-down list, select **None**.
9	Restart Messaging servers.	—	—
9a	Restart server A. • For more information, see Stopping Messaging on page 460. • For more information, see Starting Messaging on page 460.	Server A	• Stop Messaging. • Start Messaging.
9b	Restart server B. • For more information, see Stopping Messaging on page 460. • For more information, see Starting Messaging on page 460.	Server B	• Stop Messaging. • Start Messaging.
9c	Restart server C. • For more information, see Stopping Messaging on page 460. • For more information, see Starting Messaging on page 460.	Server C	• Stop Messaging. • Start Messaging.

Table continues…

No.	Task	Server or system	Required action
10	For each application server, reload User List and Global Address List Cache.	—	—
10a	On server B, reload User List and Global Address List Cache. For more information, see Loading lists on page 146.	Server B	From the **Reload Caches** heading: • Click **Reload** next to the **User List** field to load User List. • Click **Reload** next to the **Global Address List** field to load Global Address List.
10b	On server C, reload User List and Global Address List Cache. For more information, see Loading lists on page 146.	Server C	From the **Reload Caches** heading: • Click **Reload** next to the **User List** field to load User List. • Click **Reload** next to the **Global Address List** field to load Global Address List.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W