Administering Avaya Aura® Messaging

6.0
November 2011

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

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

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

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

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”). (see “Third-party Components” for more information).

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the

Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya, Avaya one-X, and Avaya Aura are registered trademarks of Avaya, Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Chapter 1: Preparing for Avaya Aura Messaging

Preparing your network

Network overview

Your IT infrastructure needs to allow inbound traffic to flow into the messaging server and outbound traffic to flow out of the Messaging server. To enable this traffic flow, you need to ensure that your network DNS record includes appropriate Messaging information.

For more information about the network topology, see the *Avaya Aura® Messaging Overview and Planning* guide.

DNS record

Avaya highly recommends that if you did not create an “A” record for the Messaging server in the Domain Name System (DNS) record, you create a CNAME record. Follow these guidelines when you create an alias:

- If you have a front-end/back-end topology, point the alias to the storage server.
- Use *avayamsg* in the alias. For example: *avayamsg.example.com*. The Messaging documentation uses this name and using a different one might confuse your users.
- Ensure that your mail gateway:
  - Can relay the fully qualified domain name (FQDN) for the storage server.
  - Can send messages to Internet domains.
  - Can grant the storage server IP access. (Some mail gateways restrict IP access.)
  - Does not require SMTP authentication. (Avaya recommends IP based restrictions.)

Preparing for Exchange forms

Exchange administration overview

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

- Verify that your Exchange server has the appropriate forms folders (libraries). If it does not, create them.
- Use Outlook to add the voice message forms to the forms folders on your Exchange server.

You can add the form to the System Folder on any of the following Exchange servers:

- Exchange 2000
- Exchange 2003
- Exchange 2007
- Exchange 2010

In large organizations with specialized administration roles, the Exchange administrator typically completes these tasks.

Supported languages

The voice messaging forms are available in the following languages.

Language	Form
Brazilian Portuguese	AvayaVoiceMessage_pt-BR.fdm
French	AvayaVoiceMessage_fr-FR.fdm
German	AvayaVoiceMessage_de-DE.fdm
Spanish	AvayaVoiceMessage_es-ES.fdm
U.S. English	AvayaVocieMessage_en-US.fdm

Exchange 2000 and 2003

Adding Organizational Forms Libraries

The following steps explain how to add an Organization Forms Library to Exchange 2000 and 2003 servers.

Procedure

1. Log on to the Exchange server.
2. Open **Exchange System Manager** and go to **Folders > System Folders**.
3. Right-click **System Folders**, and then select **View System Folders**.
4. In the folder list, double-click **EFORMS REGISTRY**.
   The **EFORMS REGISTRY** folder expands to display any existing Organizational Forms Library.
5. Determine if you need to create a new Organization Forms Library.
   You need one library for each language in your deployment.
   - If you do not need to add a new library, go to Step 10.
   - If you need to add a new library, go to the next step.
6. Right-click **EFORMS REGISTRY** and select **New > Organizational Form** from the drop-down list.
7. In the Properties dialog box, select the **General** tab and enter the following values:
   - **Name**: The name of the library. If you are deploying multiple languages, identify the language in the library name. For example: *Forms Library (en-US)*.
   - **E forms language**: The language that the forms in the library will contain.
8. Click **OK**.
   You can have only one Organizational Forms Library for each language.
9. If you need to create libraries for additional languages, repeat Step 6 through Step 8.
10. When you finish, click **OK**.

Next steps

Assign client permissions to the Organization Forms Library.

Assigning client permissions

The following instructions explain how to assign client permissions to the Organizational Forms Library on Exchange 2000 and 2003 servers.

Before you begin

- One Organization Forms Library for each language in your Messaging deployment must exist on the server. If you need to add libraries, see Adding Organizational Forms Libraries on page 7.
- You are logged in to the Exchange server.

Procedure

1. On your Exchange server, navigate to the Forms Library folder for which you want to assign client permissions.
2. Right-click on the library name and then select **Properties**.
3. In the Properties dialog box, select the **Permissions** tab, and then click **Client Permissions**.
4. If the **Name** list does not display the appropriate user account, add it.
5. If the user account does not have “Owner” permissions, grant it.
6. Click **OK**.
7. Repeat this procedure for each Forms Library in the System Folder.
8. Click **OK** to exit.

Next steps

Use the account from this procedure to log in to a computer that is running Outlook. For details, see Installing the voice message form on page 11.

Exchange 2007 and 2010

Adding Organizational Forms Libraries

The following steps explain how to add an Organizational Forms Library folder to the Public Folder on Exchange 2007 and 2010 servers.

Before you begin

If the server does not have a Public Folder, create one.

Procedure

1. Log on to the Exchange server.
2. At the Powershell prompt, run the **`get-publicfolder`** command.
3. To verify that the System Folder contains the Organizational Forms Library, run the **`get-publicfolder "\NON_IPM_SUBTREE" –recurse`** command.

   The server should return the following:

   ```
   Name : Parent Path
   NON_IPM_SUBTREE :
   EFORMS REGISTRY : \NON_IPM_SUBTREE
   <Forms Library> : \NON_IPM_SUBTREE\EFORMS
   ```

   If the System Folder contains:

   - One Organizational Forms Library, it displays under the EFORMS REGISTRY line, as shown in the above example
   - Multiple Organizational Forms Libraries, they each display on separate lines. A separate library is required for each language for which you plan to deploy the voice message form.
4. Verify that the language of the Organizational Forms Library matches the language of the voice message form. You can have only one Organizational Forms Library for each language.
5. If you need to create a new library, run the `New-PublicFolder –Path "\NON_IPM_SUBTREE\EFORMS REGISTRY" –Name "<Forms Library>"` command.

   Replace *<Forms Library>* with the name of your Organizational Forms Library. If you plan to use multiple language forms, indicate the specific language in the library name, for example *Forms Library (en-US)*.

   Repeat this step for each additional library.
6. Run the `get-publicfolder "\NON_IPM_SUBTREE" –recurse` command again to verify that Exchange created the library you just created.
7. When you are finished, enter `Exit`.

Next steps

Assign client permissions to the Organization Forms Library.

Assigning client permissions

The following instructions explain how to assign client permissions to the Organizational Forms LIbrary on Exchange 2007 and 2010 servers.

Before you begin

- The account for which you are assigning client permissions has a mailbox on the Exchange server.
- The Exchange server has one Organizational Forms Library for each language in your Messaging deployment. If you need to add libraries, see Adding Organizational Forms Libraries on page 8.

You are logged in to the Exchange server.

Procedure

1. At the Exchange Management Shell prompt, run the `Add-PublicFolderClientPermission "\NON_IPM_SUBTREE\EFORMS REGISTRY\<Forms Library>" –User "<user@domain.com>" –AccessRights "OWNER"` command.

   Replace the following command variables with your data:

   - Replace <*Forms Library*> with the name of the Organizational Forms Library that you used in Adding Organizational Forms Libraries on page 8.
   - Replace <*user@domin.com*> with a user account.
2. Record the user account information for the next procedure.
3. Repeat Step 2 and Step 3 for each Forms Library in the System Folder.
4. When you are finished, enter **Exit**.

Next steps

Use the account from this procedure to log into a computer that is running Microsoft Outlook. For details, see Installing the voice message form on page 11.

Installing the voice message form

Before you begin

- The System Folder on your Exchange server must contain one Organizational Forms Library for each language in a multilingual deployment.
- You have an account with client permissions for administering the Organizational Forms Library. See Assigning client permissions on page 10.
- You have completed either of the following:
  - Configured the avayamsg A or CNAME record in DNS. For more information, see DNS record on page 5.
  - Recorded the correct host name or IP address of a Messaging server.

About this task

Complete the following steps on any computer running Outlook.

Procedure

1. Log in with the user account that you entered into the `EFORMS REGISTRY` when you assigned client permissions.
2. Open a Web browser and go to: **http://avayamsg/download/<*VoiceMessagingFormFilename*>**. Then save the form to a temporary location on your hard drive.

   Replace *VoiceMessagingFormFilename* with the appropriate filename. See Supported languages on page 6 for a list of file names.
3. Repeat Step 2 for each language that you want to deploy.
4. Open Microsoft Outlook and select **Tools > Options**.
5. In the **General** section of the Options dialog box, click **Advanced Options...**
6. In the **Advanced Options** dialog box, click **Custom Forms...**
7. In the **Options** dialog box, click **Manage Forms...**
   In the Forms Manager dialog box:
   - The name you created for the forms library displays in the left pane.
   - The voice message form displays in the right pane.

   If you have a multilingual deployment, ensure that the language for the Organizational Forms Library and the voice message form match.
8. In the **Forms Manager** dialog box, click **Install...**
9. In the **Files of type** field at the bottom of the **Open file manager** box, select **Form Message (*.fdm)**.

10. Navigate to the voice message form file that you downloaded in Step 2. For example: `AvayaVoiceMessage_en-US.fdm`.
11. Click **Open** to install the form file.
12. In **Form Properties**, click **OK**.
13. Click **Copy** to copy the voice message form into your forms library.
14. Select **Avaya Voice Message** in the right pane and then click **Delete.**
15. If you are deploying multiple languages, repeat Step 8 through Step 14 for each language form.
16. Click **Close**.
17. Click **OK** three times to exit.

Result

When a user opens a voice message, the appropriate voice messaging form automatically downloads.

Chapter 2: Getting started with Avaya Aura Messaging

Overview

System Management Interface

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

SMI has three interfaces:

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

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

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

Administration passwords

Password security

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

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

Changing an administrator password

Each account has a default password. Avaya highly recommends that you change these default passwords the first time you log in to the Messaging system.

Procedure

1. Use the privileged administrator login and password.

   If the privileged administrator login does not exist, you must create a privileged administrator account that is part of the susers group. For more information about adding a privileged administrator account, see *Implementing Avaya Aura® Messaging*.
2. On the Administration menu, click **Server (Maintenance)** > **Security** > **Administrator Accounts**.
3. On the Administrator Accounts page, select the radio button for **Change Login**.
4. Select the log-in account from the **Select Login** drop-down list.
5. Click **Submit**.
6. Enter the new password in the **Enter password or key** field.

7. Enter the password again in the **Re-enter password or key**.
8. Click **Submit**.

Checklist for administrators

Setting up Messaging includes preparing your IT infrastructure so all of the following components can work together:

- Your network
- The Exchange server
- Your telephony server
- The Messaging storage role
- The Messaging application role
- Messaging sites and topology

The following table describes where to find initial administration tasks, who does the tasks, and on which component you do the tasks. Because IT responsibilities in large organizations may be divided among different individuals, each chapter in the table contains all the information needed by a specific administrator.

Avaya recommends that you complete the chapters in the sequence shown below.

				Where do you do it?		
No.	**Task**	**Instructions are in**	**Who does it**	**Single-server systems**	**Front-end / Back-end systems**	✔
1	Prepare the network	Chapter 1	Network administrator	—	—	
2	Load the Avaya voice messaging forms onto the Exchange server	Chapter 1	Exchange administrator	Exchange server	Exchange server	
3	Prepare the telephony server	*Supported and Unsupported Avaya Aura Messaging Integrations* on http://support.avaya.com/	Switch administrator	Telephony server	Single site: telephony server Multisite: *each* telephony server	

				Where do you do it?		
No.	**Task**	**Instructions are in**	**Who does it**	**Single-server systems**	**Front-end / Back-end systems**	✔
4	Set up the storage role	Chapter 3	Messaging administrator	Single server	Storage server	
5	Set up the application role	Chapter 4	Messaging administrator	Single server	Each application server	
6	Set up sites and topology	Chapter 5	Messaging administrator	Single server	Storage server	

Logging in to Messaging

About this task

The Messaging System Management Interface (SMI) is accessed 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:
   - Access by System Platform Web Console
     i. Log on to the System Platform Web Console.
     ii. Click **Virtual Machine Management** > **Solution Template**.

     The system displays the Virtual Machine List page.
     iii. Click the **Manage Virtual Machine** icon to select the *msg* virtual machine.
   - LAN access by IP address

     If you are logging on to the corporate LAN, type the unique IP address of the Messaging server in standard dotted-decimal notation, such as `http://192.152.254.201`.
   - LAN access by host name

     If the corporate LAN includes a DNS server that has been administered with the name of the host, type the host name, such as `http://avayamsg.example.com`.

- Laptop access by IP address

  If you are logging on to the services port from a directly connected laptop, type the unique IP address of the Messaging server in standard dotted-decimal notation, such as `http://192.152.254.201`.

3. Press `Enter`.

   Note:

   If your browser does not have a valid security certificate, you will see a warning screen and instructions to load the security certificate. If you are certain 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 S8800 Servers again, click the main menu link to **Install Avaya Root Certificate** after you log in.

   The system displays the Logon screen.

4. In the **Logon ID** field, type `craft`.
5. Click **Continue**.
6. In the **Password** field, type `crftpw`.
7. Click **Log On**.

   After successful authentication, the system displays the Messaging System Management Interface home page.

Logging out

Procedure

On any SMI page, click **Log Off**.

Chapter 3: Initial administration of the storage role

Initial administration checklist for the storage role

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

On the server running the storage role, perform the tasks in the sequence shown.

No.	SMI page	References	✔
1	Server Date/Time	Verifying the system clock on page 20	
2	Stop Messaging	Stopping Messaging on page 20	
3	Start Messaging	Starting Messaging on page 21	
4	Change LDAP Password (Storage)	Changing the LDAP root password on page 21	
5	System Status	Verifying the status of the storage role on page 22	
6	External Hosts	Administering the external SMTP host on page 22	
7	Mail Options	Adding a mail gateway on page 23	
8	Trusted Servers	Configuring a trusted server on page 23	
9	Edit Networked Machine	Setting the length of mailbox numbers on page 24	
10	Properties for New User	Adding the postmaster mailbox on page 25	
11	System Mailboxes	Configuring the postmaster mailbox number on page 26	
12	System Ports and Access	Configuring IMAP4 access on page 27	

Verifying the system clock

Messaging uses the Linux system clock to perform certain time-dependent tasks, such as placing a time stamp on voice messages and doing the nightly backup of critical system data. The clock is set during the installation of your system, but Avaya recommends that you check it when you administer your storage server for the first time. Check it again monthly and whenever a Daylight Savings Time change occurs.

Before you begin

Messaging must be running. See Starting Messaging on page 21.

About this task

Procedure

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

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

Stopping Messaging

Procedure

1. On the Administration menu, click **Messaging** > **Utilities** > **Stop Messaging**. The system displays the Stop Messaging Software page and begins a 3-minute countdown to the shutdown routine.
2. Click **Stop** if you want to begin the shutdown routine immediately.

Result

The Stop Messaging Software page refreshes periodically during the shutdown routine and displays a brief status message after **Stop Voice System info.**

Starting Messaging

Procedure

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

Result

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

Changing the LDAP root password

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

Procedure

1. Stop Messaging. See Stopping Messaging on page 20.

   For the password change to occur, Messaging cannot be running.
2. On the Administration menu, click **Messaging** > **Utilities** > **Change LDAP Password (Storage)**.
3. Select **Yes** or **No** from the **Change default LDAP Root Password** drop-down list.
4. Enter the **Old Password**.

   If you are changing the default LDAP Root Password for the first time, leave this field blank.
5. Enter the **New Password**.
6. Enter the password again in **Confirm New Password**.
7. Start Messaging. See Starting Messaging on page 21.

Verifying the status of the storage role

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

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

Procedure

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

For the status of the application role, see Verifying the status of the application role on page 222.

Enabling outbound text-based traffic

Administering the external SMTP host

Messaging uses an external SMTP relay host to forward text notifications and outbound voice messages. You enable this function by configuring the mail gateway on the External Hosts page.

Before you begin

About this task

Messaging must be running. See Starting Messaging on page 21.

Procedure

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

Configuring the **Alias** is optional.

3. Click **Save**.

Adding a mail gateway

About this task

A mail gateway enables Messaging to connect to other mail systems. It also enables the storage server to send text notifications. For more information, see Network overview on page 5.

Procedure

1. On the Administration menu, click **Messaging** > **IMAP/SMTP Settings (Storage)** > **Mail Options**.
2. In the **Maibox Gateway Machine Name** field, select the host name that you entered in Administering the external SMTP host on page 22.
3. Keep the **Server Alias** blank.
4. Click **Save**.

   For more information, see Mail Options field descriptions on page 207.

Next steps

Configure a trusted server. See Configuring a trusted server on page 23.

Configuring a trusted server

Use these instructions to identify your storage server as a trusted server within your network.

Before you begin

Messaging must be running. See Starting Messaging on page 21.

Procedure

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

The following fields get populated with AIC server information:

- Trusted Server Name: aic
- Machine Name / IP address: 127.0.0.1
- Service name: AIC
- Access to Cross domain delivery: Yes
- IMAP 4 Super User Access Allowed: Yes

4. Set **Password** and **Confirm Password** to `aicpw`.
5. Click **Save**.

   For detailed field descriptions, see Add Trusted Server field descriptions on page 58.

Next steps

Identify the length and the range of valid digits required for accessing a mailbox. See Setting the length of mailbox numbers on page 24.

Setting the length of mailbox numbers

The following instructions define the mailbox number length for all subscribers.

Before you begin

Messaging must be running. See Starting Messaging on page 21.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Server Settings (Storage)** > **Networked Servers**.
2. On the Manage Networked Servers page, select the server and then click **Edit the Selected Networked Server**.
3. In the **Mailbox Number Length** field on the Edit Networked Machine page, enter a number that corresponds to the length of the mailbox extension used by your system.
4. In the **MAILBOX NUMBER RANGES** table, enter the prefix and the range of mailbox numbers for Messaging.

   Enter a range of numbers that conforms to the number you selected in the **Mailbox Number Length** field. For example, if you selected 5 from the list, then enter a 5–digit number, and if you selected 8, then enter an 8–digit number.

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

The following example shows the range for a 5–digit mailbox number.

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

For more information, see Add Networked Machine field descriptions on page 65.

5. Click **Save**.

Next steps

See Adding the postmaster mailbox on page 25.

Adding the postmaster mailbox

The postmaster is responsible for managing the mail for the site and answering questions about users. The postmaster mailbox is a system-wide mailbox set aside for the postmaster. Use these instructions to create a postmaster mailbox.

Before you begin

Messaging must be running. See Starting Messaging on page 21.

Procedure

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

   The length of the mailbox number and extension must match the length that you specified in Setting the length of mailbox numbers on page 24.
4. Set **MWI enabled** to no.
5. Turn off the following defaults:

- **Include in Auto Attendant directory**
- **User must change voice messaging password at next logon**

6. Complete the following password fields. See Password security on page 14 for guidelines for setting passwords:
   - **New password**
   - **Confirm password**
7. Click **Save**.
   The system creates a site-wide mailbox.

Next steps

Define the mailbox that you just created as the postmaster mailbox. See Configuring the postmaster mailbox number on page 26.

Configuring the postmaster mailbox number

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

Before you begin

Ensure that:

- You have created a mailbox for the postmaster. See Adding the postmaster mailbox on page 25.
- Messaging is running. See Starting Messaging on page 21.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **System Mailboxes**.
2. In the **Internet Postmaster Mailbox Number** field, enter the postmaster mailbox number.
3. Click **Save**.
   The system does not count the postmaster mailbox that you just created against the total number of subscriber licenses that your organization has purchased.

Next steps

Enable IMAP4 ports. See Configuring IMAP4 access on page 27.

Configuring IMAP4 access

You set system-wide parameters on the System Ports and Access page. Use the following instructions to give the storage server access to the IMAP4 server and, therefore, the capability to communicate with remote clients.

Before you begin

Messaging must be running. See Starting Messaging on page 21.

Procedure

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

   For more information, see System Ports and Access field descriptions on page 61.
3. Click **Save**.

Next steps

Administer the application role. See Initial administration checklist for application roles on page 30.

Chapter 4: Initial administration of the application role

Deployment scenarios

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

Each of the following deployment scenarios refers to the tasks in Initial administration checklist for application roles on page 30. For more information about your deployment options, see the *Avaya Aura® Messaging Overview and Planing* guide.

One server and one site

In this scenario, you need to associate one application role with one site. You do this by completing the first six tasks in the checklist. You can skip the remaining tasks.

Multiple servers and one site

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

For this example, you would complete:

- Tasks 1 through 8 on the first application server
- Tasks 1 and 9 on the second and third application servers

Multiple servers and multiple sites

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

For example, if your topology is:

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

In the first site, Atlanta, you would complete:

- Tasks 1 through 8 on the first application server
- Tasks 1 and 9 on the second and third application servers

In the second site, Boston, you would complete the first six steps.

Important:

Do not restore system files that you backed up for one site onto application servers associated with a different site. Each site requires site-specific settings such as dial plans and extension lengths.

Initial administration checklist for application roles

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

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

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

Perform the tasks in the sequence shown.

No.	SMI page	Task	Do on first application server of first site?	Do on first application server of subsequent site?	Do on subsequent server in any site?
1	Telephony Integration	Integrating with the telephony server on page 32	Yes	Yes	Yes
2	Dial Rules	Setting up extension length for dial rules on page 35	Yes	Yes	No
3	Dial Rules	Defining dial rules on page 36	Yes	Yes	No
4	Attendant	Assigning an attendant number on page 37	Yes	Yes	No
5	System Parameters	(Optional) Enabling fax on page 38	Yes	Yes	No
6	Language Packs	Configuring languages on page 39	Yes	Yes	No

No.	SMI page	Task	Do on first application server of first site?	Do on first application server of subsequent site?	Do on subsequent server in any site?
7	AxC Address	Changing the AxC IP address on page 40	Yes	No	No, if multi-server topology
8	Backup Now	Backing up application files on page 41	Yes	Yes	No
9	View/Restore Data	Restoring application files on page 42	No	No	Yes

Telephony integration

Integration requirements

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

Telephony parameters

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

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

Network parameters

You also need the following information for each application server:

- Port number, typically 5060 for TCP transport or 5061 for TLS transport
- Domain name

Integrating with the telephony server

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

Before you begin

Complete all the tasks in the Initial administration checklist for the storage role on page 19.

Gather the parameters from the telephony server that are required for integration. See Integration requirements on page 31.

Procedure

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

   For more information, see Telephony Integration field descriptions on page 32.
3. Click **Save**.

Next steps

- If you are administering the first (or the only) application role for a site, go to Setting up extension length for dial rules on page 35.
- If you have completed all of the administration and backup tasks for the first application role in a multiserver topology and you want to administer another application role, go to Restoring application files on page 42.

Telephony Integration field descriptions

Basic configuration:

Name	Description
Switch Number	The default is 1. Do not change it unless directed to do so by Avaya Support.
Extension Length	The extension length must match the dial plan of the telephony server. The range is 3–10.
Switch Integration Type	Messaging uses SIP integration.
Quality Of Service	This information is only relevant if your IP network infrastructure supports the Quality of Service feature. You can accept the default values or enter new ones. However, the

Name	Description
	values must match the number in the network region of the telephony server that is used by the Messaging signaling group. The range for both fields is 0–63. • Call Control PHB sets the quality of service level for call control messages. • Audio PHB sets the quality for audio streams.
UDP Port Range	The range of port numbers used by the User Datagram Protocol (UDP) for the Real Time Protocol (RTP). The default range is 8000 through 10000. • You can change the **Start** value. • The system uses the number of available trunks to calculate the **End** value. You must ensure that the range of ports that you allocate to UDP does not conflict with ports used for other purposes.

SIP Specific configuration:

Name	Description
Transport Method	The transport method the telephony server uses for SIP signaling. The transport method of the application server and the telephony server must match. Choices are: • TCP (not encrypted). Use port 5060. • TLS (encrypted). Use port 5061.
Far-end Connections	The total number of SIP proxy servers. Valid far-end connections are: • Direct (no proxy). Select 1. • Session Manager. Select a maximum of 12. • SIP Enablement Services. Select 1. • AudioCodes gateway. Select a maximum of 4. • Other application servers for the same site The number of **Connection** fields expand to match the number you select.
Connection x	The IP address and port number for each far-end connection. If you select more than one far-end connection, the system accepts incoming calls from any of the servers on the connection list. It attempts to place outgoing calls to the first server that accepts a connection in the order listed. MWI only uses one connection regardless of how many sites or servers are in your deployment.

Name	Description
Messaging Address	The IP address for this near-end application server is always a read-only field. The port number is typically one of the following: • TCP = 5060 • TLS = 5061
SIP Domain	The domain names for the application server and the far-end connection must match. Example: sip.example.com
Messaging Ports	The number of network ports reserved for Messaging: • The Call Answer Ports range is 2–100 • The read-only Transport field displays the number of ports available for transfer operations. This number is the difference between the number of trunks and the number of call answer ports. A typical ratio between call answer and transfer ports is 80:20. If you need help, click **Show Capacity Calculator**.
Switch Trunks	The number of trunk members for messaging on the telephony server. If the telephony server is configured for multiple signal groups, enter the sum of all trunk members in all groups. • The minimum is the number of call answer ports plus one. • The maximum is the sum of the number of call answer and transfer ports. Avaya recommends that you do not exceed 120 switch trunk members. The **Transfer Ports** field is a read-only field. The system uses the following formula to calculate the number of transfer ports: Switch Trunks Total – Call Answer Ports = Transfer Ports. The number in the **Switch Trunks Total** field must match the number of trunk members on the telephony server.
Media Encryption	The type of Secure Real-time Transport Protocol (SRTP) media encryptions that the switch uses. This field is optional.

Dial rules

Setting up extension length for dial rules

Important:

If your deployment includes more than one server in the application role, only define the extension length for dial rules on the first server in the site. You administer the servers for subsequent application roles by backing up the first application role and then restoring the data onto the server for the subsequent application role. Refer to the Initial administration checklist for application roles on page 30 for information about which procedures you do manually on the server and which ones are done automatically through the backup and restore process.

Before you begin

Before you set the extension length on an application server, you must have previously set it on the storage server. See Integrating with the telephony server on page 32.

Procedure

1. On the Administration menu, click **Messaging** > **Server Settings (Application)** > **Dial Rules**.
2. Under the **Company DID numbers that should be treated as internal numbers** heading, enter a number in the **Number of digits in an extension** field.

   The number you enter must match the number in the **Extension Length** field on the Telephony Integration page and the **Extension length** field on the Sites page. If you do not remember this number, click on **Messaging > Switch Link Administration**.
3. Click **Apply**.

   For more information, see Dial Rules field descriptions on page 70.

Next steps

- If you are administering the first (or the only) application role for a site, go to Defining dial rules on page 36.
- If you are administering additional application servers that support the *same* site as the first server, go to Restoring application files on page 42.

Defining dial rules

The application role uses dial rules for the following features:

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

Important:

If your deployment includes more than one server in the application role, only define dial rules on the first server in the site. You administer the servers for subsequent application roles by backing up the first application role and then restoring the data onto the server for the subsequent application role. Refer to the Initial administration checklist for application roles on page 30 for information about which procedures you do manually on the server and which ones are done automatically through the backup and restore process.

Before you begin

If you are administering the first (or only) application role, you must first complete the procedure for Setting up extension length for dial rules on page 35.

Procedure

1. On the Administration menu, click **Messaging** > **Server Settings (Application)** > **Dial Rules**.
2. Fill out the fields under the following headings:
   - **This Location**
   - **Dial-Out Settings**
   - **Company DID numbers**
   - **PBX Caller ID Information**

   You can define advanced dialing rules later. For more information, see Dial Rules field descriptions on page 70.
3. Click **Apply**.

Next steps

- If you are administering the first (or the only) application role for a site, go to Assigning an attendant number on page 37.
- If you are administering additional application servers that support the *same* site as the first server, go to Restoring application files on page 42.

Assigning an attendant number

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

Important:

If your deployment includes more than one server in the application role, only assign an attendant number on the first server in the site. You administer the servers for subsequent application roles by backing up the first application role and then restoring the data onto the server for the subsequent application role. Refer to the Initial administration checklist for application roles on page 30 for information about which procedures you do manually on the server and which ones are done automatically through the backup and restore process.

Before you begin

If you are administering the first (or only) application role, you must first complete the procedure for Defining dial rules on page 36. Do not repeat this task on additional application servers that support the *same* site as the first server.

Procedure

1. On the Administration menu, click **Messaging** > **Server Settings (Application)** > **Attendant/Operator**.
2. In the **Schedule type** drop-down list, select one of the following:
   - not available (the default)
   - full-time

   If you change the default, the system displays the **Attendant (operator) extension** field.
3. In the **Attendant (operator) extension** field, enter the extension of the attendant.

   If you do not enter an extension number, when the caller presses 0 Messaging tells the caller that no operator is available and disconnects the call.
4. In the **General delivery mailbox number** field, enter the extension for a shared mailbox that is accessible by all attendants.

   If you entered an extension number in the **Attendant (operator) extension field** and if the attendant does not answer, then the system transfers the caller to this mailbox.
5. Click **Apply**.

Next steps

- If you are administering the first (or the only) application role for a site, go to Enabling fax on page 38.
- If you are administering additional application servers that support the *same* site as the first server, go to Restoring application files on page 42.

Enabling fax

Messaging integrates with a third-party fax server. Follow these instructions only if your organization plans to provide fax capabilities to its users.

Important:

If your deployment includes more than one server in the application role, only enable fax on the first server in the site. You administer the servers for subsequent application roles by backing up the first application role and then restoring the data onto the server for the subsequent application role. Refer to the Initial administration checklist for application roles on page 30 for information about which procedures you do manually on the server and which ones are done automatically through the backup and restore process.

Before you begin

- If you are administering the first (or only) application role, you must first complete the procedure for Assigning an attendant number on page 37.
- Your IT network must include a fax server.

Procedure

1. On the Administration menu, click **Messaging** > **Server Settings (Application)** > **System Parameters**.
2. Fill out the fields under the **Fax Server** heading.

   See System Parameters field descriptions on page 78.
3. Click **Apply**.

Next steps

- If you are administering the first (or the only) application role for a site, go to Configuring languages on page 39.
- If you are administering additional application servers that support the *same* site as the first server, go to Restoring application files on page 42.

Configuring languages

You can install language packs and select the languages for your site on the Languages page. You can download additional language packs from http://support.avaya.com. The languages you select on this page are used by the following system features:

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

Important:

If your deployment includes more than one server in the application role, only configure languages on the first server in the site. You administer the servers for subsequent application roles by backing up the first application role and then restoring the data onto the server for the subsequent application role. Refer to the Initial administration checklist for application roles on page 30 for information about which procedures you do manually on the server and which ones are done automatically through the backup and restore process.

Before you begin

About this task

If you are administering the first (or only) application role, you must first complete the Enabling fax on page 38 procedure. Do not repeat this task on additional application servers that support the *same* site as the first server.

Procedure

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

   For more information, see Language Packs field descriptions on page 77.
3. Click **Apply**.

Next steps

- If you are administering the first (or the only) application role for a site, go to Changing the AxC IP address on page 40.
- If you are administering additional application servers that support the *same* site as the first server, go to Restoring application files on page 42.

Changing the AxC IP address

Avaya ships Messaging servers that are set up for a single-server topology. If this is your topology, you can skip this procedure.

The 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. However, if you have a topology with more than one server, you must change the default AxC IP address on *each* dedicated application server.

Important:

If your deployment includes more than one server in the application role, only change the AxC IP address on the first server in the site. You administer the servers for subsequent application roles by backing up the first application role and then restoring the data onto the server for the subsequent application role. Refer to the Initial administration checklist for application roles on page 30 for information about which procedures you do manually on the server and which ones are done automatically through the backup and restore process.

Before you begin

- Administer the storage role. See Initial administration checklist for the storage role on page 19.
- If you are administering the first (or only) application role, you must first complete the procedure for Configuring languages on page 39. Do not repeat this task on additional application servers that support the *same* site as the first server.

Procedure

1. On the Administration menu, click **Messaging** > **Advanced** > **AxC Address**.
2. In the **AxC IP address** field, enter the IP address of the storage server.
3. In the **AxC port** field, change the default to `80`.
4. Click **Apply**.

Next steps

- If there is only one application server for your site, you are ready to define your site and topology. Go to Initial administration checklist for sites and topology on page 45.
- If there are more application servers for your site, you must configure each of them so they are *identical* to all others in the cluster. You can accomplish this by backing up the application server you just configured and restoring the data on each of the other application serves. Go to:
  - Backing up application files on page 41

- Restoring application files on page 42

Backing up application files

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

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

Before you begin

Before backing up the application role, ensure that:

- Your IT network includes an FTP server for storing the backed-up data.
- You have completed all administration tasks for the first (or only) application role. See the Initial administration checklist for application roles on page 30.
- Messaging is not running. See Stopping Messaging on page 20.

Procedure

1. On the Administration menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Backup Now**.
2. Under the **Data Sets** heading, select **Messaging Application**.
3. Under the **Backup Method** heading, select **Network Device** and then choose a location for the backed-up files by completing the following fields:
   - **Method**
   - **User Name**
   - **Password**
   - **Host Name**
   - **Directory**

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

   For more information, see Backup Now field descriptions on page 148.

Next steps

Restore the backed-up data set on to any additional application servers for the site. See Restoring application files on page 42.

Restoring application files

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

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

Before you begin

Before restoring previously backed-up data sets to subsequent application servers:

- Integrate each subsequent application server for a site with your telephony server. See Integrating with the telephony server on page 32.
- Ensure that you have the information that you entered on the Backup Now page.
- Ensure that Messaging is not running. See Stopping Messaging on page 20.

Procedure

1. On the Administration menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **View/Restore Data**.
2. Under the **View current backup contents in** heading, select **Network Device**. Then use the same information that you used when you backed up the data to complete the following fields:
   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 **Apply**.
5. Repeat these steps for each additional application server.
6. Restart Messaging.

Next steps

If you have additional application roles to administer for your site, repeat these instructions on each additional application server. When you finish, administer your site and topology. See Initial administration checklist for sites and topology on page 45.

Chapter 5: Sites and topology

Initial administration checklist for sites and topology

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

Avaya recommends that you complete the tasks in the sequence shown below.

			Where do you do it?		
No.	**SMI page**	**Task**	**Single-server systems**	**Front-end / Back-end systems**	✔
1	Sites	Setting site properties for the first time on page 46	Single server	Storage server	
2	Sites	Adding additional sites on page 47	Single server	Storage server	
3	Topology	Adding the first application server on page 51	Single server	Storage server	
4	Topology	Adding additional application servers on page 52	—	Storage server	
5	Cluster	Configuring a cluster on page 53	—	Each application server in the cluster	
6	System Operations	Verifying the link to the AxC on page 56	Single server	Each application server in the cluster	

Initial site administration

Overview for administering sites for the first time

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

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

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

Setting site properties for the first time

If you are the administrator who first sets site properties, you are also tasked with ensuring that Messaging is working properly. This may mean that decisions about whether to enable Auto Attendant and the wording of the system greeting have not yet been made. You can set these properties later, but you must at least set the Main Properties.

About this task

Your Messaging system comes with a site named Default. You need to change this name and enter information about your organization's primary messaging mailbox.

Complete the following instructions on the storage server.

Procedure

1. On the Administration menu, select **Messaging** > **Messaging Administration** > **Sites**.
2. Complete the fields under the **Main Properties** heading.

   For more information, see Sites field descriptions on page 47.
3. (Optional) If your organization has decided to enable Auto Attendant, complete the fields under the **Auto Attendant** heading. 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 under the **Auto Attendant Greeting / Menu** heading. 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

- If you want to add additional sites to your network, go to Adding additional sites on page 47.
- If you do not want to add another site, go to Overview for administering topology for the first time on page 50.

Adding additional sites

About this task

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

Complete the following instructions on the storage server.

Procedure

1. On the Administration menu, click **Messaging** > **Messaging Administration** > **Sites**.
2. On the Sites page, click **Add New...**
3. Enter appropriate information in the fields.

   For more information, see Sites field descriptions on page 47.
4. Click **Save**.

Next steps

Define your system topology. See Overview for administering topology for the first time on page 50.

Sites field descriptions

Name	Description
Site	The drop-down list displays all of your Messaging sites. You can add a new site or delete an existing site by selecting the appropriate button.
Name	The name of the site. Messaging comes with a site named Default. You change this name

Name	Description
	when you set site properties for the first time.
Main Properties	
Messaging access number (external)	The external telephone number that users dial to access their mailbox. Also called the external pilot number. The telephony server includes this number in the text notifications that it sends to mobile phones or pagers. The e-mail client sends it in e-mail notifications. Typically, you enter this number without any formatting, for example: *2125551234*. This number must match the corresponding number in the voice mail hunt group on the telephony server. The General page in User Preferences displays it for the user.
Messaging access number (internal)	The internal telephone number that users dial to access their mailbox. Also called the internal pilot number. This number is typically shorter than the external number. The General page in User Preferences displays it for the user.
Extension length	The length of extensions for users on this site.
Mailbox length	The length of mailbox numbers for users on this site. The number in this field must match the number in the **Mailbox Number length** field on the Networked Machine page.
Non-Uniform Dial Plan Handling (Optional)	
Prefix	The digits before the telephone number that indicate an action to the telephony server. For example, if you dial zero in front of a long distance telephone number in the U.S., the telephony server connects you to an operator at the telephone company.
Country code	The number that precedes the national number in an international phone call.
Use leading zero in global number	Indicates if the dialing plan uses leading zeros.
Auto Attendant	
Auto Attendant	Enables the Auto Attendant feature. The default is *disabled*.

Name	Description
	The Auto Attendant can transfer callers to local extensions.
Auto Attendant pilot number	Designates the pilot number for the Auto Attendant.
Additional sites included in the directory	The name of another site *with the same dialing plan* in a multisite deployment. The default is *None*. By default, a user is associated with only one site. And all users that are associated with a given site are included in the Auto Attendant directory for that site. When you enter the name of another site in this field, users who are in either directory can reach each other through the Auto Attendant for this site. Each site has its own Auto Attendant directory. By default, all users associated with a given site are included in the Auto Attendant directory for that site. When you are deploying a multisite Messaging environment, you create a system-wide Auto Attendant directory when you enter the name of another site. In a multisite deployment, a site's Auto Attendant directories can be added to other sites Auto Attendant directories. To add another Auto Attendant directory from a different site, click Add, and select the additional site. The box below Auto Attendant Directory shows the additional Auto Attendant directories added to the site.
Keypad entry	Defines the keypad options: • **BASIC**: Only extension • **ENHANCED**: Extension and spell mode Both options include speech recognition if the **Speech recognition** field equals *enabled*.
Speech recognition	Enables speech recognition. The default is *disabled*. Speech recognition is a licensed feature. Do not enable this feature unless your Messaging license includes a license for Speech recognition.

Name	Description
	When you enable speech recognition, callers can speak a name that is in the Auto Attendant directory and the Auto Attendant will transfer the call to that person.
Auto Attendant Greeting / Menu	
Initial greeting	The greeting that Auto Attendant plays to a caller. You can browse to a pre-recorded .wav file.
Menu (speech recognition disabled):	The menu that Auto Attendant plays when the **speech recognition** field is set to *disabled*.
Menu (speech recognition enabled):	The menu that Auto Attendant plays when the **speech recognition** field is set to *enabled*.

Initial topology administration

Overview for administering topology for the first time

The topology of a Messaging system is the relationship between the application servers and the sites they support. You define this relationship on the Topology page. This page:

- Lists the sites that you previously defined on the Sites page
- Assigns an application server to a site
- Allows you to change the topology by adding or deleting application servers

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

- In a single-server topology, you manage application and storage roles on the same server
- In a front-end/back-end topology, you 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.

capacityportredundancy**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.

Clustering application servers allows you to:

- Increase the system capacity so it 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. Application servers within a cluster are configured identically and are, therefore, interchangeable.

Important:

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

Adding the first application server

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

- Only application server for the site
- First of several application servers for the site

Complete this procedure on the storage server.

Note:

Only assign *one* site to an application server.

Before you begin

- Configure the storage and one or more application servers. See *Chapter 3: Initial administration of the storage role* and *Chapter 4: Initial administration of the application role*.
- Create a site with one or more application servers. See Overview for administering sites for the first time on page 46.
- Ensure that all application servers that you plan to add to the topology are running.

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **Topology**.
2. When the Topology page opens for the first time, it defaults to the IP address of the storage server. Delete this IP address as follows:
   a. Under the **Remove Application Server** heading, select the IP adddress for the storage server from the drop-down list for the **IP address** field.
   b. Click **Remove**.
3. Under the **Add Application Server** heading:
   a. In the **IP address:** field, enter the IP address of the first application server.

b. In the **Role in application server cluster?** field, select **Add as stand-alone (non-clustered) application server or as the first application server in a new cluster**.

4. In the **Sites / Application Servers** table, select **Active** from the drop-down list next to the site that this application server will support.
5. Click **Update**.

Example

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

Sites / Application Servers

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

Next steps

- If there is only one application server for your site, you are ready to administer users on the system.
- If there are more application servers for your site, you must add them to the system topology so they can recognize each other. See Adding additional application servers on page 52.

Adding additional application servers

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

Before you begin

- Install and configure all application servers that you plan to associate with the site. See *Chapter 4: Initial administration of the application role*.
- Add the first application server to the site. See Adding the first application server on page 51.
- 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. Under the **Add Application Server** heading:

a. In the **IP address:** field, enter the IP address of the application server you are joining to the cluster.

b. In the **Role in application server cluster?** field, select **Form (or join) a cluster by joining existing application server:**

c. From the drop-down list, select the application server that you want to join.

clustertime zone
All application servers in a cluster are identical, so you can select any server in the list.

You can join up to four application servers to form a cluster. However, all servers in a cluster must be in the same time zone.

3. Click **Add**.
The system:

   - Adds the server you identified in Step 2a to the **Sites / Application Servers** table
   - 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 joins the application servers into one or more clusters, depending on your entries.

Next steps

Configure a cluster of application servers. See Configuring a cluster on page 53.

Configuring a cluster

You must add all the application servers that you joined together into a cluster to each other's cluster list. This list enables them to recognize each other. You configure these lists on each individual application server.

Before you begin

About this task

Define the application server as a member of the cluster. See Adding additional application servers on page 52.

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** box expands to match the number you entered.
3. In each **Member** field, enter the IP address of an application server.
   - For a new cluster member, add each of the other cluster members to its cluster list.
   - For each preexisting cluster member, add the new member to its cluster list.

   Do not change the information in the **Disk usage quota** field.
4. Click **Apply**.
5. Continue repeating these steps until you configure all application servers for all of your sites.

Topology field descriptions

Name	Description
Sites / Application Servers	The table displays the following information about the sites that you created on the Sites page: • The name of the site • The IP address of each application server associated with this storage server • The application server that is associated with a site as the *active* server The system updates the table after you add or remove application servers.
Add Application Server	
IP address	The IP address of the application server you want to add to Messaging.
Role in application server cluster	Your options are to:

Name	Description
	• **Add as stand-alone (non-clustered) application server or as the first application server in a new cluster:** Select this option to add the first application server to a site. • **Form (or join) a cluster by joining existing application server:** Select this option to add an application server to a site that already has an existing application server associated with it. You can add up to four application servers to a cluster. All application servers in a cluster are identical, so you can select any existing application server in the drop-down list that is associated with the site. Remember to cluster the added server with the existing ones. See Configuring a cluster on page 53.
Remove Application Server	
IP address	The IP address of the application server you want to remove from the site.

Cluster field descriptions

Settings	Description
Cluster Members	Any number from 1 through 4. The maximum number of application servers in a cluster is 4.
IP address of each appliance	One 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** field.
Disk usage quota	This is an advanced setting and Avaya recommends that you consult your account representative before you enter data into this field.

Verifying the link to the AxC

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

- User List
- Global Address List

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

Before you begin

Complete Step 1 through Step 5 in the Initial administration checklist for sites and topology on page 45.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Advanced (Application)** > **System Operations**.
2. Under **Reload Caches**, click **Reload** for each of the following lists:
   - User List
   - Global Address List

   If the caches reload without error, the application role is connecting to the AxC and the storage role properly. If the system returns an error message, make sure that:
   - You have entered the IP address for the AxC correctly. See Changing the AxC IP address on page 40.
   - You have set up the topology correctly. See Overview for administering topology for the first time on page 50.
3. If required, repeat Step 1 and Step 2 until the caches reload without error.
4. Repeat this procedure on each server with the application role.

Chapter 6: Managing servers

Storage servers

Adding a trusted server

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

Procedure

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

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

   For more information, see Add Trusted Server field descriptions on page 58.
5. Click **Save**.

Manage Trusted Servers field descriptions

Name	Description
Trusted Server	The name of each trusted server.
IP Addr/Name	Depending on how the server was administered, either the IP address or the machine name of each server.

Name	Description
Service Name	The service name of the trusted server.

Add Trusted Server field descriptions

Name	Description
Trusted Server Name	The name for the server can be up to 64 characters long and must start with a letter. Other characters can be letters, numbers, dashes (-), and underscores (_). This field is mandatory.
Password	The password the server uses to connect to Messaging.
Confirm Password	Confirmation of the **Password**.
Machine Name / IP Address	Either the host name or the valid 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 **Search Order** field on the Network Addressing page. • Trusted servers that use the private LAN require a valid IP address.
Service Name	A descriptive name that indicates the use of this trusted server. The system automatically populates this field if you select a type of trusted server from the **Special Type** drop-down list.
Minutes of Inactivity Before Alarm	The number of minutes the trusted server can be inactive before the system raises a minor alarm. The default is 0. If you do not change the default, the system does not check for inactivity from this trusted server.
Access to Cross Domain Delivery	Specifies whether you want to allow cross-domain delivery through this trusted server.
Special Type	The type of trusted server. The system automatically populates or restricts some of the fields on the page based on your selection.

Name	Description
LDAP Access Allowed	Specifies whether you want this 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 this trusted server and the storage server. This field is disabled when the value in the **LDAP Access Allowed** field is *no*. Your choices are: • **Must use SSL** to require Secure Sockets Layer (SSL) encryption. SSL is the preferred encryption method because it provides full channel encryption. • **Must use SSL or encrypted SASL** to require either SSL or Simple Authentication and Secure Layer (SASL) encryption. • **No encryption required** is the default.
IMAP4 Super User Access Allowed	Specifies whether you want IMAP4 super user access to the storage server from this trusted server. The default is *no*.
IMAP4 Super User Connection Security	The type of encryption for the IMAP4 super user connection between this trusted server and the storage server. This field is disabled if the **IMAP4 Super User Access Allowed** field is *no*. Your choices are: • **Must use SSL** to require SSL encryption. SSL is the preferred encryption method because it provides full channel encryption. • **Must use SSL or encrypted SASL** to require either SSL or SASL encryption. This choice is the default.

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.

Name	Description
Service Name	The service name of each trusted server.

Setting Messaging parameters

Procedure

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

   For more information, see System Ports and Access field descriptions on page 61.
3. Click **Save**.

Privacy enforcement

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

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

Setting the privacy enforcement level for IMAP4 clients

About this task

To select the privacy enforcement level for IMAP4 and POP3 clients:

Procedure

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

System Ports and Access field descriptions

Fields	Description
SYSTEM ATTRIBUTES	
System Prime Time Start	The starting time, in hours and minutes, for the prime time interval for collecting data for traffic and other features that use the prime time interval. This is normally the time that your company opens for business. The default is 08:00.
System Prime Time End	The ending time, in hours and minutes, for the prime time interval. This is normally the time that your company closes. The default is 17:00.
Maximum Simultaneous LDAP Directory Update Sessions	The maximum number of simultaneous LDAP sessions allowed during a full remote update. When the maximum is reached, an administrator cannot request a full remote update until one of the sessions is finished. The default is 100.
IMAP4 TUI Password	The password used for the IMAP4 communication between systems.
Confirm IMAP4 TUI Password	A confirmation of the **Confirm IMAP4 TUI Password** entry.
Default Internet Subscriber Community	Do not use this field.
Privacy Enforcement Level	If the sender marks a message private, then the recipient can not forward it from the Telephone User Interface. The options are:

Fields	Description
	• *Voice* enforces privacy from the TUI. • *Email* requests that the recipient keeps the message private.
RESCHEDULING INCREMENTS FOR FULL MAILBOX DELIVERY	
Increment fields	The intervals in days, hours, and minutes that the system waits to attempt to resend messages that it could not deliver on the previous attempt due to a full mailbox. When the system uses the last increment specified, the message is marked as nondeliverable. You can specify a maximum of 10 rescheduling increments.
SYSTEM TCP/IP PORTS	
LDAP SSL Port	The state of the primary LDAP port. You cannot modify the primary port number. • *Disabled* only disables authenticated and anonymous access for the corporate LAN. • *Authenticated Only* enables authenticated access and disables anonymous access on the corporate LAN. • *Authenticated & Anonymous* enables both authenticated and anonymous access on the corporate LAN. Changing the state of the LDAP port temporarily interrupts the corporate LAN access to LDAP.
LDAP Port	The port number for the LDAP SSL Port. The default is 636. If you change the port number, you must restart the system.
LDAP Internal Server Port	The port that the LDAP server uses for internal processes. You cannot disable this port. The default is 55389. If you change the port number, you must restart the system.
LDAP Directory Update Port	The port that the directory update LDAP server uses. The default is 56389.
LDAP Front End Alternate Port	An optional, secondary port for LDAP. The port is automatically enabled when you enter a port number. The default is blank. If you change the port number, you must restart the system.

Fields	Description
IMAP4 TUI Port	You cannot change the status of this port. The port is disabled and the port number is 55143.
IMAP4 Port	The port that the IMAP4 server uses for IMAP4 communication with remote clients. If you select *Enabled*, enter the port number to be used by the IMAP4 server.
IMAP4 SSL Port	The port that the IMAP4 server uses for IMAP4 SSL communication with remote clients. If you select *Enabled*, enter the port number to be used by the IMAP4 server. The default is 993.
POP3 Port	The port that the POP3 server uses for POP3 communication with remote clients. • *Enabled* allows the use of POP3 clients for e-mail messaging. • *Disabled* blocks POP3 e-mail client access to the messaging server. If you select *Enabled*, enter the port number to be used by the POP3 server for POP3 communication with remote clients. The default is 110.
POP3 SSL Port	The port that the POP3 server uses for POP3 SSL communication with remote clients. • *Enabled* allows POP3 clients to use the POP3 SSL port for more secure access. • *Disabled* blocks POP3 SSL client access. If you select *Enabled*, enter the port number to be used by the POP3 server for POP3 SSL communication with remote clients. If you enable POP3 SSL, subscribers might need to configure their e-mail clients to use SSL. The default is 995.
SMTP Port	The port that the SMTP server users for SMTP communication with remote clients. If you select *Enabled*, enter the port number to be used by the SMTP server. The default is 25. Disabling this port only disables access for the public LAN. If you change the port number, you must restart the system.
Allow TLS for Outgoing SMTP	Enable or disables outgoing SMTP attempts to use Transport Layer Security (TLS) to encrypt the SMTP conversation.

Fields	Description
SMTP Alternate Port	The port that the SMTP server uses for SMTP SSL communication with remote clients. If you select *Enabled*, enter the port number to be used by the SMTP server for SMTP SSL communication. The default is 465. If you change the port number, you must restart the system. If you enable SMTP SSL, subscribers might need to configure their e-mail clients to use SSL.
SMTP SSL Port	The port that the SMTP server use for SMTP communication with remote clients. This is an additional port that can be used on the public network instead of the traditional SMTP port. The port is automatically enabled when you enter a port number. The default is blank.
MCAPI Port	The port that the MCAPI server uses. The default is 55000. If you change the port number, you must restart the system.

Adding a network server

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

About this task

The following instructions assume that you are adding an LDAP server.

Procedure

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

   For more information, see Add Networked Machine field descriptions on page 65.
5. Click **Save**.

Manage Networked Servers field descriptions

Name	Description
Server Name	The name of each networked server.
IP Address	The IP address of the networked server.
Server Type	The type of server. For all but the local machine, the server type is LDAP.
ID	The numerical identification of this server.
Total Subs	The number of susbcribers associated with this network server.

Add Networked Machine field descriptions

Name	Description
Machine Name	The name of the server you want to add.
Password	The LDAP password used for directory updates.
Confirm Password	Confirmation of the**Password** entry.
IP Address	The IP address of the server you want to add.
Machine Type	The Server Type for the server you want to add. For all but the local machine, the server type is LDAP.
Mailbox Number Length	The length of the mailbox number must match the mailbox number length specified for the site.
Default Community	Do not use this field.
Updates In	Specifies whether the local server accepts directory updates from this network server. If you are administering the local server, this field controls updates on a system-wide basis.

Name	Description
	• *yes* accepts directory updates from network servers. • *no* blocks directory updates to this sever, regardless of the setting of this field for the network server.
Updates Out	Specifies whether the local server can send updates about users to the specified remote server. If you are administering the local server, this field controls updates on a system-wide basis.
Remote LDAP Port	The port that the system uses to connect to this network server in order to send directory updates. The default is the port specified in the **LDAP Directory Update Port** field on the System Ports and Access page.
Inbound LDAP Security	The type of encryption required for the connection between the storage server and a remote network server for inbound LDAP directory updates. When you set the **Updates In** field to *no*, the system denies any attempt by a remote network server to update the LDAP directory without using the specified level of security. Options are: • *Must use SSL* requires SSL encryption for inbound LDAP directory updates • *Must use SASL or SSL* requires either SASL or SSL encryption for inbound LDAP directory updates The default is *Must use SASL or SSL*.
Outbound SMTP Port	The port the system uses to connect to this network server. The defaults are port 25 for SMTP and port 465 for Secure SMTP.
Outbound SMTP Service	The type of SMTP service required for the connection between the storage server and a remote network server. Choices are SMTP or Secure SMTP.
MAILBOX NUMBER RANGES *The total length of the prefix and mailbox number cannot exceed 64 digits.*	
Prefix	The prefix for the range of telephone numbers for users on this server. The system uses the prefix to distinguish between

Name	Description
	servers that have overlapping ranges for mailbox numbers.
Starting Mailbox Number	The first number in the range for mailbox numbers on this server. The number of digits in the range must match the entry in the **Mailbox Number Length** field. Unless you have a specific reason for excluding some ranges, start with 1 preceded by leading zeros. Example for a 5–digit number: *00001*.
Ending Mailbox Number	The last number in the range. Example for a 5–digit number: *99999*.
Telephone Number Mapping *When a local user receives a call-answer message, the system attempts to match the sender's calling party number (CPN) to a user number in the database.*	
Enable Telephone Number Mapping	• *yes* tells the system to use a lookup table to map the CPN for the sender to the number for the recipient. • *no* tells the system not to identify the recipients as users in the messaging network. If you change this option from *yes* to *no*, the system removes all previously defined mapping from the local database. It also sets the telephone numbers for all existing users associated with the network server to null.
Map From	The system compares the digit string that you enter in this field to the base numbers for a user. A match occurs when the value in the **Map From** field is the same as the beginning portion of the base number. When this happens, the system creates a mapped telephone number by: • Stripping the matching digits from base number, and then • Prepending the number in the **Map To** field to the base number. If the **Map From** field is empty, the system compares incoming CPNs to all base numbers. Valid values are digits from 0 through 50.

Name	Description
	You can add more than one set of Map From and Map To numbers. If you do, the sets can differ in length.
Map To	The digits string that the system prepends to the base number after it strips the digits that match the **Map From** field. When the **Map To** field is: • Empty, the system does not prepended digits to the base number after any digit stripping takes place. • *none*, the system sets the matching telephone number to null. The Map To entries can be different lengths. The resulting telephone numbers must be no more than 50 digits long.
Add Mapping	The mapping to add to the mapping table.
Delete Mapping	The mapping to delete from the mapping table. To change an existing mapping, delete it and then create a new one.

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 each network server. Also called Machine Type. For all but 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

This 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 this report.
Log End Date	The date of the last entry in the log used to generate this 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** shows the last time the local server made a connection to the remote server. • **Incoming Connections** shows the last time the remote server made a connection to the local server.
Status	The status of the last connection.
Retries	The number of consecutive times that the local server tried, but failed, to connect to the remote server.

Report of Server Ranges field descriptions

Name	Description
Machine 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

Configuring dial rules settings

Before you begin

Changes in the Dial Rules page must be applied before the editable rules scripts in the Advanced Rules panel are made available. For more information, see Configuring advanced dial-out rules on page 72.

Note:

Dial Rules updates must be applied to all application servers.

Procedure

1. On the Administration menu, click **Messaging** > **Server Settings (Application)** > **Dial Rules**.
2. On the Dial Rules page, verify that the information provided in the following sections match the properties of the telephony server that is connected to this application server.
   - **This Location**
   - **Dial-Out Settings**
   - **Company DID numbers that should be treated as internal numbers**
3. Modify the details, if required.

   For more information, see Dial Rules field descriptions on page 70.
4. Click **Apply**.

Dial Rules field descriptions

Name	Description
This Location	
Country code	The country code for the location of the application server. This number is used to

Name	Description
	determine whether calls are internal, local, domestic, or international. The default is *1*.
Area code / Private number	The area code and private number for the location of the application server. Example: *212 -5551212* The system uses: • The area code to determine if outgoing calls are local or long distance. • The private number to determine if incoming calls include a local extension that is in the Global Address List. The typical format of the private number is *main number + local extension*.
Dial-Out Settings	
Long-distance prefix	The default is 1.
International prefix	The default is 011.
Outside line prefix	The default is 9.
Company DID numbers that should be treated as internal numbers	
Number of digits in an extension	Must match the number in the **Extension Length** field on the Telephony Integration page.
Number of DID ranges	The number of Direct Inward Dialing (DID) ranges for internal numbers. The system uses DID ranges to route inbound calls to extensions within the bounds of the range.
PBX Caller ID Information	
Caller ID Internal Number Prefix	The dial-out prefix for internal calls. Used only when required by the telephony server for caller ID.
Advanced Rules	
Dial-out rules	Click **Edit Dial-Out Rules** to customize the dial-out rules.
Dial-in rules	Do not change advanced dial-in rules unless directed to do so by Avaya Client Services.

Configuring advanced dial-out rules

Dial-out rules define the dial strings that are sent to the telephony server for making calls. You need to verify the required information in each step of the following procedure before you proceed to the next step.

Before you begin

- Verify that the information on the Dial Rules page is correct. For more information, see Configuring dial rules settings on page 70.
- Backup the existing dial rules script into Notepad or a similar application.

Procedure

1. **How many digits are required to call a number within the originating area code?**

   North American area codes typically require either 7 or 10 digits.

   - 7: No changes are needed. Go to the next step.
   - 10 or other: Scroll to `LocalCallNumLength = 7` and change `7` to the correct number of digits. For example, `10`.

2. **Will users be allowed to make calls to toll-free numbers?**

   - Yes: No changes are needed. Go to the next step.
   - No: Scroll to `TollFreeAreaCodes`

     ```
     var = new Array("800", "888", "877", "866")
     ```

     Delete everything between the parentheses, as shown below:

     ```
     var TollFreeAreaCodes = new Array( )
     ```

3. **Does any of the Class of Service definitions use the dial-out privilege level “Local“?**

   - Yes: Go to the next step.
   - No: Go to Step 6.

4. **Is the area code of the telephony server the only local area code?**

   - Yes: Go to the next step.
   - No: Scroll to `LocalAreaCodes`

     ```
     var LocalAreaCodes = [phoneAreaCode]
     ```

     Enter additional area codes separated by commas. (The area code for the telephony server is included in the variable `phoneAreaCode`.)

For example, after you add area codes 650 and 510, the variable looks like the following line of code.

```
var LocalAreaCodes = [phoneAreaCode, 650, 510]
```

5. **Are all calls placed to the area codes in Step 4 (including the area code for the telephony server) local calls?**

   - Yes, all calls are local:

     Scroll to `LocalPortionOfLAC`:

     ```
     var LocalPortionOfLAC = portionSomeCalls
     ```

     Change the assigned value to `portionAllCalls`:

     ```
     var LocalPortionOfLAC = portionAllCalls
     ```

   - No, only some calls are local:

     Scroll to `LocalCallRanges`:

     ```
     var LocalCallRanges = new Array ( // EXAMPLE: new LocalCallRange(650,
     653, 657) )
     ```

     For each area code in Step 4, create a list of all the prefixes (NXX) or prefix ranges that are local calls. Enter each range in a new `LocalCallRange` declaration, separated by commas, within the assignment of `LocalCallRanges`. Each `LocalCallRange` declaration requires an area code, a start prefix (NXX), and an end prefix (NXX). For example, if these are local calls:

     - (408) 123-XXXX
     - (408) 251-XXXX through (408) 258-XXXX
     - (650) 335-XXXX through (650) 345-XXXX
     - (510) 756-XXXX

     then edit the lines as follows:

     ```
     var LocalCallRanges = new Array ( new LocalCallRange(408, 123, 123),
     new LocalCallRange(408, 251, 258), new LocalCallRange(650, 335, 345),
     new LocalCallRange(510, 756, 756) )
     ```

6. **Does your organization use DID numbers?**

   - Yes: Go to the next step.
   - No: Go to Step 9.

7. **Does the telephony server handle calls to DID numbers correctly (i.e., dial them as internal calls to an extension)?**

   - Yes: Go to the next step.
   - No, Messaging should dial the extension (“downgrade” the number):

Scroll to `DowngradeDID`.

```
var DowngradeDID = false
```

Change the value to `true`:

```
var DowngradeDID = true
```

Next, scroll to `DIDRanges`:

```
var DIDRanges = new Array (
```

Create a list of all the dial inward dial (DID) phone number ranges. For each range, enter the area code, and the starting and ending DID numbers in a new `DIDRange` declaration, separated by commas, within the `DIDRanges` declaration. For example, if these are the DID numbers:

- (408) 961-5730 to 961-5749
- (408) 961-3020 to 961-3040
- (408) 200-5110 to 200-5150
- (510) 123-4560 to 123-4567

then change the `DIDRanges` as follows:

```
var DIDRanges = new Array ( new DIDRange(408, 9615730, 9615749), new
DIDRange(408, 9613020, 9613040), new DIDRange(408, 2005110, 2005150),
new DIDRange(510, 1234560, 1234567) )
```

8. **Does the customer want all numbers that start with the international prefix (e.g. 011) to be classified as international, or as invalid (rejected)?**

   - As international numbers: Go to the next step.
   - As invalid numbers (rejected by the system):

     Scroll to `InternationalIfStarts011`:

     ```
     var InternationalIfStarts011 = true
     ```

     Change the value to `true`:

     ```
     var InternationalIfStarts011 = false
     ```

9. **Does the customer want all numbers which can't be classified as internal, local, long distance, or international to be classified as invalid (rejected) or as international?**

   - As invalid numbers (rejected by the system): Go to the next step.
   - As international numbers:

     Scroll to `InternationalIfNoOther`:

     ```
     var InternationalIfNoOther = false
     ```

     Change the value to `true`:

     ```
     var InternationalIfNoOther = true
     ```

10. **Sometimes users do not include the area code of the telephony server when they enter phone numbers. Does the customer want the system to prepend the area code to these numbers or do they want the system to classify these numbers as invalid and reject them?**

    - Prepended with local area code: Go to the next step.
    - Classified as invalid numbers (rejected by the system):

      Scroll to `MissingAreaCodeAction`:

      ```
      var MissingAreaCodeAction = macUseLocalAreaCode
      ```

      Change the value to `macRejectAsInvalid`:

      ```
      var MissingAreaCodeAction = macRejectAsInvalid
      ```

11. Go to the **Dial-Out Test Numbers** section.

    Define the various test numbers as you expect your users to enter in their User Preferences for Reach Me, Notify Me, and Personal attendant features.

    Then click **Test** to verify how the current dial-out settings handle the entered numbers.

    - **Input Phone Number**: Number as listed in the test number pane
    - **Call Type**: Classifies the number so that the system can evaluate whether the associated user has the required dial-out privilege in their COS. The results here are related to the COS privileges as follows:

Call Type	Required Minimum Dial-out Privilege in COS
INTERNAL	OnPremise
LOCAL	Local
LONGDISTANCE	LongDistance
INTERNATIONAL	International
INVALID	*not applicable, number will not be dialed*

    - **Output Phone Number** - dial string that the Messaging server will offer to the telephony server (as defined in the Switch Link Admin page).

    If the results are not as expected, revisit the settings in earlier steps.

    If you are satisfied with the results, click **Save** to save the test numbers and the rules.

Configuring languages

You can install language packs and select the languages for your site on the Languages page. You can download additional language packs from http://support.avaya.com. The languages you select on this page are used by the following system features:

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

Important:

If your deployment includes more than one server in the application role, only configure languages on the first server in the site. You administer the servers for subsequent application roles by backing up the first application role and then restoring the data onto the server for the subsequent application role. Refer to the Initial administration checklist for application roles on page 30 for information about which procedures you do manually on the server and which ones are done automatically through the backup and restore process.

Before you begin

About this task

If you are administering the first (or only) application role, you must first complete the Enabling fax on page 38 procedure. Do not repeat this task on additional application servers that support the *same* site as the first server.

Procedure

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

   For more information, see Language Packs field descriptions on page 77.
3. Click **Apply**.

Next steps

- If you are administering the first (or the only) application role for a site, go to Changing the AxC IP address on page 40.
- If you are administering additional application servers that support the *same* site as the first server, go to Restoring application files on page 42.

Language Packs field descriptions

Name	Description
Language Packs: Installed Languages table	
Name	A list of all installed language packs. The default is American English (en-US).
User Selectable	The language for User Preferences and the TUI. If you install multiple languages, users can select the one they prefer.
Language Settings	
System Language	The language that a caller hears. The language used by Auto Attendant and call answering.
Default Subscriber UI Language	The language of the user interface. If you install multiple languages, users can select the one they prefer.
Language Packs	
Current Application software release	The version number of the Messaging system.
Add Language Pack	Browse to the location of the language packs that you want to add to this application server.

Configuring system parameters

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

You can preset all these parameters with default values, and for the most part, the system invokes these defaults without further modification requirements. However, as the administrator, you can change these parameters as necessary. If you choose to change them, be sure to 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 appropriate information in the fields as described in System Parameters field descriptions on page 78.
3. Click **Apply**.
4. Repeat this procedure on each application role in the cluster.

System Parameters field descriptions

Name	Description
Voice Messages	
Include caller ID in subject line	Possible values are: • *Enabled* (default) includes the Caller ID in the subject line of voice messages. • *Disabled* excludes the Caller ID in the subject line. Only select *Disabled* when the switch integration does not support Caller ID.
Intro text in subject line of original messages	The textual prefixes to the subject line of voice messages. The type of prefix that the system uses depends on the message context: • Original messages • Message replies • Forwarded messages The text content is the Caller ID and contact name.
Intro text in subject line of message replies	
Intro text in subject line of forwarded messages	
Call Sender	
For internal calls, a call attempt times out after	The number of seconds that elapses before the telephony server sends an internal call that was initiated from Call Sender to voice mail. The default is 16 seconds. This value should be less than the time it typically takes a call to a local extension to roll over to voice mail in RNA. If the time out value is configured at the system level on the telephony server, you may be able to check your telephony server for a typical setting.

Name	Description
For external calls, a call attempt times out after	The number of seconds that elapses before the telephony server sends an external call that was initiated from Call Sender to voice mail. The default is 45 seconds. During Call Sender initiated calls, to avoid the caller going to voice mail, the time out value for Call Sender should be lower than the typical time it takes for calls to an external phone numbers to roll over to voice mail in RNA cases.
Maximum duration of a Call Sender initiated call	The maximum duration of a call, in seconds, when placing a call using Call Sender. The default is 10800 seconds (3 hours).
Recording Times	
Maximum voice message length	The maximum time for a message recording measured in seconds. The default is 1200 seconds (20 minutes).
End-of-recording silence	The seconds of silence that indicates the end of recording. The default is 4 seconds.
VoIP DTMF cut-off time	For VoIP integrations only, this is the number of milliseconds to cut off at the end of a recording that has been terminated by DTMF. The default is 150 milliseconds.
Play on Phone	
Time out (on no answer) after	If a Play on Phone call is not answered in the specified time, in milliseconds, the system terminates the call. Choose a duration that is one ring less than the number of rings for call forwarding defined on the PBX or switch. The default is 16000 milliseconds.
Reach Me	
Number of seconds per ring for "Reach Me"	For the Reach Me feature, the number of seconds a ring is presumed to take when calculating how long to wait before timing out and going to the action. The default is 5 seconds.
Ringback Timeouts	
First ringback timeout	The time to wait, in milliseconds, for first ringback to occur. The default is 15000 milliseconds.
Ringback timeout	Time to wait, in milliseconds, for ringbacks to end. The default is 7000 milliseconds.

Name	Description
Nightly Maintenance	
Maintenance time	The scheduled time for nightly maintenance of each application server. During maintenance time, the local directory cache in the application server gets refreshed with a fresh copy of the directory cache.
Fax Server	
Fax Server pilot number	The number (typically a hunt group number) of the third party fax server to which faxes should be forwarded. Example: 6300.
Fax detection time	The duration (in milliseconds) the application server listens to possible fax tones after accepting a call. The default is 20000.
Identification for Fax Transfer	Fax recipient identification user property defining either a mailbox, primary extension, or work phone number. The default is Mailbox.
DTMF to send after the transfer to the fax server	Can be empty or “*” “#”. The default is (empty).

Changing the configuration of a cluster

About this task

Use the following steps to add or delete servers with the application role from an existing cluster. To set up a cluster for the first time, see Configuring a cluster on page 53.

Procedure

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

   For more information, see Cluster field descriptions on page 55.
3. Click **Apply**.

Cluster field descriptions

Settings	Description
Cluster Members	Any number from 1 through 4. The maximum number of application servers in a cluster is 4.
IP address of each appliance	One 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** field.
Disk usage quota	This is an advanced setting and Avaya recommends that you consult your account representative before you enter data into this field.

Changing attendant settings

About this task

Use the following steps to change existing settings for the attendant schedule, main extension, and general-delivery voice mailbox. To set up an attendant for the first time, see Assigning an attendant number on page 37.

Note:

You must make the same changes on *each* server with the application role. If you do not, the system will overwrite your changes the next time it performs a backup and restore.

Procedure

1. On the Administration menu, click **Messaging** > **Server Settings (Application)** > **Attendant/Operator**.
2. Select a **Schedule Type**.
3. Specify **Attendant (operator) Extension**.
4. Specify **General delivery mailbox number**.
5. Click **Apply**.

For information on the fields, see Attendant / Operator field descriptions on page 82.

6. Repeat this procedure on each server with an application role.

Attendant / Operator field descriptions

Field	Description
Schedule type	Defines the availability of the attendant or live operator. The options are: • Not available • Full-time
Attendant (operator) extension	Defines the extension of the attendant, or live operator. If a caller presses 0 to reach the operator, the system transfers the caller to this extension. When a caller reaches a mailbox that has a *personal attendant*, however, pressing `0` routes the caller to the extension for the personal attendant instead. If you select Not available in the **Schedule type** field, the Attendant / Operator page does not disply this field.
General delivery mailbox number	Defines the voice messaging mailbox that callers reach when the attendant or live operator does not answer incoming calls. Typically, this is a shared mailbox accessible by all *live* operators. A typical greeting for this mailbox is: "There is no one available at this time" . You can leave this field blank if you do not want callers directed to a voice mailbox.

External servers

Changing external SMTP hosts

About this task

When you administered the storage role for the first time, you integrated Messaging with an external SMTP host server and a mail gateway. The external SMTP host forwards outbound e-mail and is required to support notifications. The mail gateway enables Messaging to connect to other mail systems.

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

Procedure

1. To change the external SMTP host server, see Administering the external SMTP host on page 22.
2. To change the mail gateway, see Adding a mail gateway on page 23.

Chapter 7: Managing users

User overview

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 page to add, modify, or delete a local user or an info mailbox.
- *Remote* users are served by a voice mail domain that is different than 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. Typically, they exchange messages with each other regularly.

User options for responding to messages

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

- Send a reply message.
- Call the user who left the message.
- Generate an e-mail as a response to the message if Notify Me is enabled for the user.

The availability of these 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 rulesfor replying to messages

Dial rules

Dial rules determine how local users can respond to messages from callers. Different rules may apply for remote users and for callers who are not members of your organization. For example, local users may be able to return a call from a remote user by replying to a Call Answer message but they must dial the telephone number of other callers.

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

See Defining dial rules on page 36.

mapping tables

Mapping tables

Mapping tables enable your local system to send messages from a local user to a remote extension. They are used to convert the telephony server extensions or network addresses of remote users to telephone numbers that your local system can recognize. These telephone numbers are then shared between all messaging systems in your voice mail network.

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

You create the mapping tables when you add a network server to your system. See Adding a network server on page 64.

remote updatesupdateremote user list

Remote updates

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

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

For more information, see About remote updates on page 96.

Managing local users

Adding users

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. Under the Add a new user heading on the User Management page, click **Add**.
3. Enter appropriate information in the fields.
   For more information, see User Management > Properties field descriptions.
4. Click **Save**.

If appropriate, you can designate the user as an attendant. See Assigning an attendant number on page 37.

5. Repeat Step 2 through Step 4 for each additional user.
6. Notify the new users that the messaging service is available.

Changing user properties

About this task

You can view and modify the properties of users who have previously been added to the 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 is changed 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 can not access this system-generated ID.

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **User Reports**.
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 page. However, this page does not have filters that assist you in locating a specific user.
3. On the User Management > Properties page, modify the user information as appropriate.

   For more information, see User Management > Properties field descriptions.
4. Click **Save**.

Deleting users

Procedure

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

You can also delete users from the User Management page. However, this page does not have filters that assist you in locating a specific user.

3. On the User Management > Properties page, click **Delete**.

   For information about the fields, see User Management > Properties field descriptions.

User Management field descriptions

Name	Description
License Status	
License mode	Available modes are: • *Normal*. The system also displays the following status information: the license name, how many licenses users have acquired a license, and how many total licenses your organization has purchased. • *Restricted*. The system also displays information about the restriction. • *Error* indicates that you are in the grace period for new licenses.
Edit User / Info Mailbox	
Identifier	The mailbox number for the user whose user properties you want to edit.
Add User/Info Mailbox	
Add a new user	The Add button opens the User Management > Properties for New User page.
Add a new Info Mailbox	The Add button opens the User Management > Properties for New Info Mailbox page.

User Management > Properties field descriptions

Name	Description
User Properties	

Name	Description
First name	The first name of the user. There is no default value.
Last name	The last name of the user. This field is required. There is no default value.
Display name	The name that Messaging displays during communications.
Site	The name of the site for which the user is a member. For more information about sites, see Sites overview.
Mailbox number	The mailbox number for the user. All mailbox numbers must be unique.
Internal Identifier	The internal identifier of the user. This field only displays if you are editing an existing user.
Extension	The telephone extension of the user. The length of the extension must match the length that is set for the site and for the telephony integration for the application servers that are associated with the site. See the following for more information: • Sites field descriptions on page 47 • Integrating with the telephony server on page 32 Typically, the extension is unique. However, if it is shared with another user, Messaging presents the name of both users and prompts callers to select the desired mailbox.
Include in Auto Attendant directory	Adds the user to the Auto Attendant directory. See Sites field descriptions on page 47.
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 extension needs to be maintained in the internal directory.
Class of Service (COS)	The Class of Service (COS) for the user. Select the COS from the drop-down list. The COS controls user access to many features and provides general settings, such as mailbox size. For more information, see Class of Service overview on page 99.
Pronounceable name	The name of a user, info mailbox, or distribution list may not follow the pronunciation rules of the primary language for your system. To increase the likelihood

Name	Description
	that the Speech Recognition feature will recognize the name, spell the name the way you would pronounce it. For example, if the primary language of your system is English, spell Dan DuBois `Dan Doobwah`. You can also enter an alternative name for the user. For example, William Bell may also be known as Bill Bell. If you enter `William` in the **First name** field, `Bell` in the **Last name** field, and `Bill Bell` in the **Pronounceable name** field, the speech engine will recognize both William Bell and Bill Bell.
MWI enabled?	Enables the message waiting indicator light (MWI) feature. Typically, select • *Yes* when the user has a desktop telephone • *No* when the user only has a voice mailbox • *ByCOS* when the Class of Service controls how MWI is enabled This field overrules the MWI setting defined by the COS for which the user is associated.
New password	The password the user must use to log in to the Messaging mailbox. If you leave this field blank for an existing user, the password does not change.
Confirm password	Confirmation of the **New Password**. You only need to complete this field if you are adding a new password or changing an existing password.
User must change voice messaging password at next logon	Forces users to change their passwords the next time they call in to their voice mailboxes. By default, Messaging requires that new users change their temporary passwords when they log in to their mailbox for the first time.
Voice messaging password expired	Allows the continued use of an expired user password. Messaging only enables this option if a user password expires. Clear the check box to allow the user to continue using the password.
Locked out from voice messaging	Locks the user out of the system. Messaging automatically locks the system when the user fails to enter proper login credentials after a certain number of consecutive failed attempts. The **Lock out users after** field on the System Policies page determines the number of allowable consecutive failed attempts.

Name	Description
	Clear the check box to give the user access to the system.

Configuring System Policies

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

Procedure

1. Use a privileged user account and password to log in to the server that is running the storage role.
2. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **System Policies**.
3. On the System Policies page, enter appropriate information.
   For more information, see System Policies field descriptions on page 91.
4. Click **Save**.

System Policies field descriptions

Name	Description
Password Policy	
Minimum password length	Minimum number of characters required for a password.
Maximum password length	Maximum number of characters for a password.
User passwords expire	Number of days after which the password expires.
Warn users	The number of days before the current password expires and the day the system starts sending the user a warning to change their password.
Lock out users after	Number of failed login attempts before the system locks the user account.
Caller Applications Administrator	

Name	Description
Password	Password for accessing Caller Applications Editor
Confirm password	Password for accessing Caller Applications Editor

Managing info mailboxes

Info mailbox overview

An info mailbox can play a greeting and provide information to a caller. Examples of the content of an info mailbox include:

- Directions to your location
- Your business hours
- Weather or road conditions
- School enrollment or closing announcements
- Human resources announcements

Other facts about info mailboxes are:

- A caller can not leave a message in an info mailbox.
- The name of the info mailbox in the Auto Attendant directory is a Text-to-Speech playback of the display name.
- *Info Mailbox* is the default name of the Class of Service that controls the maximum length of a recorded message in an info mailbox.
- The default for the maximum length of a message in an info mailbox is 5 minutes. You can change this default on the Class of Service page. See Changing a Class of Service on page 100.

Adding an info mailbox

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.
2. Click the **Add** button below **Add a new Info Mailbox**.

3. Enter appropriate information in the fields.

   For more information, see Properties for New Info Mailbox field descriptions on page 93.

4. Click **Save**.

Next steps

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

Properties for New Info Mailbox field descriptions

Name	Description
First name	The first name of the info mailbox to be added or modified. This field has no default value.
Last name	The last name of the info mailbox to be added or modified. This field is required and has no default value.
Display name	The display name of the info mailbox. The name that Messaging displays during communications.
Site	The name of the site for which the info mailbox is a member. For more information about sites, see Sites overview.
Mailbox number	The mailbox number for the info mailbox. All mailbox numbers must be unique.
Internal Identifier	The e-mail address of the info mailbox. This field only displays if you are editing an existing user.
Extension	The telephone extension of the info mailbox. The length of the extension must match the length that is set for the site and for the telephony integration for the application servers that are associated with the site. See the following for more information: • Sites field descriptions on page 47 • Integrating with the telephony server on page 32

Name	Description
Include in Auto Attendant directory	Adds the mailbox in the Auto Attendant directory. See Sites field descriptions on page 47.
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 extension needs to be maintained in the internal directory.
Class of Service (COS)	The Class of Service (COS) for the info mailbox, typically *Info Mailbox*. The COS controls user access to many features and provides general settings, such as mailbox size. For more information, see Class of Service overview on page 99.
Pronounceable name	The name of an info mailbox may not follow the pronunciation rules of the primary language for your system. To increase the likelihood that the Speech Recognition feature will recognize the name, spell the name the way you would pronounce it. For example, if the primary language of your system is English, spell Dan DuBois `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 will recognize both names.
After the Greeting Plays	The action Messaging takes after it plays the greeting. The options are: • *Hang up* • *Transfer to* the mailbox number that you enter
New password	The password the user must use to log in to the Messaging mailbox. If you leave this field blank for an existing info mailbox, the password does not change.
Confirm password	Confirmation of the **New Password**. You only need to complete this field if you are

Name	Description
	adding a new password or changing an existing password.
User must change voice messaging password at next logon	Forces users to change their passwords the next time they call in to the info mailbox. By default, Messaging requires that new users change their temporary passwords when they log in to their mailbox for the first time.
Voice messaging password expired	Allows the continued use of an expired user password. Messaging only enables this option if a user password expires. Clear the check box to allow the user to continue using the password.
Locked out from voice messaging	Locks the user out of the system. Messaging automatically locks the system when the user fails to enter proper login credentials after a certain number of consecutive failed attempts. The **Lock out users after** field on the System Policies page determines the number of allowable consecutive failed attempts. Clear the check box to give the user access to the system.

Managing remote users

Types of remote users

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

- Administered remote users are users whom you have defined as remote users within the local system. You define remote users when you:
  - Conduct remote updates. See About remote updates on page 96 for more information.

- Manually administer a remote user instead of waiting for a remote update. See Running a remote update manually on page 98 for more information.

- Unverified remote users are remote users who 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 are remote users who appear in the local database only because they have successfully exchanged messages with the local system.

About remote updates

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

- You to automatically add all remote users who need to exchange messages across the network
- Your local messaging system to exchange user information with each remote messaging systems that is administered on the local system

Remote updates greatly reduce the time required to set up the messaging digital network. Whether you use the remote updates feature depends on the:

- Number of users in your network
- Size and disk space of your local system
- Number of networking ports that you are using

You also can enter remote user information manually. Before you administer your user or remote update information, consult with the remote system administrators in your network. Each remote system administrator must determine whether to use remote updates.

Types of remote updates

The following types of remote updates are available:

- Complete updates
- Partial updates

Complete updates

Complete updates exchange all user information between all systems. When you add a new system to the network, each existing system must request a complete update from the new system to add the new users to the network. Complete updates might involve thousands of users and require heavy system resources. Therefore, Avaya strongly recommends that you perform complete updates during non-prime time to reduce the impact on system users.

Additionally, the local messaging system can automatically schedule a complete update during non-prime time from a remote system if the local system detects discrepancies among databases.

Partial updates

Partial updates occur on a regular basis to add or change information for users. For example, a partial update occurs when a new user is added to a remote system or a local system.

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

Setting up remote updates

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

Before you begin

- The administrator for each remote system has agreed to allow remote updates from your local system.
- Your local server is connected to at least one remote server. See Adding a network server on page 64.

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 details of each server are displayed on the Manage Networked Servers page.
2. Select the server you want enable for remote updates.
3. Click **Edit the Selected Networked Server**.
4. Enable the **Update In** and **Update Out** fields.

   For more information,Add Networked Machine field descriptions on page 65.
5. Click **Save**.
6. Repeat this procedure on each networked server that you want to receive remote updates.

Viewing the remote users report

About this task

You can view remote user information on the User Reports page.

Procedure

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

For more information, see Reports field descriptions on page 198.

Running a remote update manually

About this task

You can run a remote update manually if you need to populate the user database quickly or correct database inconsistencies that were discovered during an audit.

Note:

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

Procedure

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

   Tip:

   Click **Refresh Update Status** to verify the status of the update.
8. Return to the Messaging Measurements page and confirm the number of remote users.
9. Repeat Step 2 through Step 4.
10. On the Administration menu, click **Messaging** > **Logs** > **Administrator**.
11. On the Administrator's Log page, click **Display** and verify that no conflicts or problems occurred with the remote update.

Chapter 8: Class of Service

Class of Service overview

A Class of Service (COS) defines the privileges and the features assigned to a group of users.

- Use the Class of Service page to define each COS, create new COSs, and change or rename existing COSs.
- Use the User Management page to assign a previously defined COS to a user.

Default Classes of Service:

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

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

  You create an info mailbox, when you follow the instructions for Adding an info mailbox on page 92. You cannot create an info mailbox by assigning the Info Mailbox COS to the user.
- *Administrator* allows you to send system broadcast messages. A typical system broadcast message contains announcements or instructions from the system administrator about the voice mail system. This COS is unrelated to the administrative privileges handled through the Server (Maintenance) RBAC administration.
- ELA allows you to use the Enhanced-List Application.

For more information, see Class of Service field descriptions on page 101.

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 page, click **Add New**.
3. Enter appropriate information in the Class of Service page.

   For more information, see Class of Service field descriptions on page 101.
4. Click **Save**.

Changing a Class of Service

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. Select the Class of Service that you want to change from the **Class of Service** drop-down list.
3. Make your changes.

   For information about the fields on this page, see Class of Service field descriptions on page 101.
4. Click **Save**.

Deleting a Class of Service

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. Select the Class of Service that you want to delete from the **Class of Service** drop-down list.

3. Click **Delete**.
4. Click **OK** on the system prompt.

Class of Service field descriptions

Name	Description
Class of Service	The name of the Class of Service (COS) that you are adding or editing.

distribution listbroadcast messagespasswordaging**General:**

Name	Description
Name	Your customized name for the COS. This name is a convenience to you. A descriptive name might be more helpful than a number.
User can send to system distribution lists (ELAs)	Allows the user to send messages via Enhanced-List Application (ELA) distribution lists. See Enhanced-List Application overview on page 109 for more information about ELAs.
Recognize and forward fax messages (to external fax server)	Enables fax for this COS.
Dial-out privilege	Indicates the types of calls users in this class are allowed to make when using the Call Sender, Play on Phone, Reach Me and Notify Me features. Possible values are None, On Premise, Local, Long Distance, and International.
Set Message Waiting Indicator (MWI) on user's desk phone	For users with an MWI lamp on their desk phone, the lamp lights up when an unheard message is in their inbox.
Enable password aging	Indicates whether users must periodically change their passwords. If users do not change their passwords within a specific amount if time, the passwords expires and Messaging blocks the user from services until an administrator resets the passwords. The default is to disable password aging. You:

Name	Description
	• Set the aging parameters on the System Policies page. See Configuring System Policies on page 91. • Reset expired passwords by clearing the **Voice messaging password expired** field on the User Management > Properties page. See Changing user properties on page 87.
User can send system broadcast messages	Indicates whether a user can send system broadcast messages. A typical system broadcast message contains announcements or instructions from the system administrator about the voice mail system.

greetings**Greetings:**

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

Name	Description
Normal greetings a user can record	Number of greetings a user can record. The options are: • None • One greeting (same greeting for busy and no-answer) • Two greetings (different greetings for busy and no-answer)
Maximum length	The maximum number of seconds for a greeting.
User can record extended absence greeting	Specifies whether users can record an Extended Absence Greeting (EAG). Callers cannot dial-through an EAG.
Block message recording if extended absence greeting is recorded	Blocks callers from leaving a message if the user has activated EAG.

Notify MeoutcallingnotificationUser PreferencesNotify Me**Notifications:**

The fields under the Notifications heading give users access to notification features. Each notification feature that you enable on the Class of Service page displays on the Notify Me page in User Preferences. Features that you do not enable are hidden from the user.

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

Name	Description
Allow text message (or page) notification	Enables the system to send a text notification to a mobile phone or pager in order to notify the user that a new voice message was delivered to their mailbox. If allowed: • You must provide the e-mail address for the appropriate SMS gateway. See Adding mobile operators on page 105. • Users must enable the Notify Me settings within their personal User Preferences.
Allow outcalling notification	Enables outcalling. Outcalling alerts a user to new messages by having the system place a call to that user. Outcalling requires that the user has appropriate dial-out privileges.
Maximum number of rings	The maximum number of times the phone that the user has designated as the outcall phone rings before the system hangs up during an outcall attempt. The range is 1 to 10. This field is disabled if **Allow outcalling notification** is No.
Start after	The length of the delay between the time a user receives a message (time stamp) and the first outcall attempt. The range is 0 minutes to 24 hours.
If no-answer or busy, retry after	The length of the delay between an unsuccessful outcall attempt and a new outcall attempt. (The called phone may be unanswered or busy.) The range is 0 minutes to 24 hours.
Stop after	The length of the delay between the time the message was received (time stamp) and when outcall attempts are terminated. The range is 0 minutes to 24 hours.
Allow email notification	Enables the system to send a text message to an e-mail address in order to notify the user that a new voice message was delivered to their mailbox. Options are:

Name	Description
	• Yes, with or without recording • Yes, only without recording • No If allowed, users must *also* enable the Notify Me settings within their personal User Preferences.

storagemessagesmessage storage**Message Storage:**

The fields under the Message Storage heading control the amount of space that each user has on the message store.

Name	Description
Maximum storage space	The maximum storage space allocated to an individual user.
Max Call Answer Length	The maximum duration of call answer messages a user can receive.

message retention**Message Retention:**

The fields under the Message Retention heading control how long the system stores messages for the user.

Name	Description
Unread messages in Inbox folder	The number of days unread messages are stored in the Inbox folder. Options are: • Keep messages forever. • Delete messages after the specified number of days.
Read messages in Inbox folder	The number of days read messages are stored in the Inbox folder. Options are: • Keep messages forever. • Delete messages after the specified number of days.
Messages in other folders	Users with IMAP access to their mailbox can create folders in addition to their Inbox folder. This setting controls the number of days messages are stored in a folder that the user creates. Options are:

Name	Description
	• Keep messages forever. • Delete messages after the specified number of days.

Adding mobile operators

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

The Web site for each mobile operator typically provides information about the mail gateway. Other Web sites provide a world wide list of mobile operators that contains this information. Avaya does not guarantee the accuracy or completeness of the information on these Web sites. It is your responsibility to verify the correctness of the information.

Note:

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

Before you begin

About this task

Gather 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. Under the **Notifications** heading on the Class of Service page, set the **Allow text message (or page) notification** field to *Yes*.
3. Click the **Mobile Operators** link.
4. Enter the appropriate information in the **Mobile Operators Definitions for Text Message Notifications** table.

   For more information, see Mobile Operators field descriptions on page 106.
5. Click **Save**.

Next steps

Test the mail gateway for each mobile operator that you plan to support. See Testing mail gateways on page 106.

Testing mail gateways

Before you begin

- Complete the instructions for Adding mobile operators on page 105.
- Provide a test phone or pager for each mobile operator that you added to the Mobile Operators page.

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **Class of Service**.
2. Under the **Notifications** heading on the Class of Service page, click the **Mobile Operators** link.
3. Ensure that the e-mail gateway address for mobile operator that you want to test is listed in the **Mobile Operator Definitions for Text Message Notifications** table. If it is not, see Adding mobile operators on page 105.
4. Enter the appropriate information in the fields under the **Test** heading.

   For more information, see Mobile Operators field descriptions on page 106.
5. Click **Send**.
6. Validate that the mobile device received the test message.

Mobile Operators field descriptions

Name	Description
Internal ID	A unique identifier that describes the mobile operator. This name is internal to your organization and will be *invisible* to users.
Description	The name of the operator. This name will be *visible* to users.
Address template	The part of the e-mail address that the operator uses that is the same for all users. The system substitutes *{0}* with the number for the user. The system uses the number from the Mobile phone or page field on the User Preferences, General page.

Name	Description
	If you need to add a prefix, put the prefix in front of the {0} variable.
Mobile phone (or pager) number	The phone or pager number of the test device
Mobile operator	The name of the mobile operator for the e-mail address you want to test. The drop-down list displays the name that are in the **Description** field.
Message	Any text that you want to send to your test device .

Chapter 9: Distribution lists

Enhanced-List Application overview

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

Implementation prerequisites

Before you implement ELA, collect the following information:

- An available Class of Service (COS) number. (The default for ELA is 8.) ELA uses this COS number for list mailboxes and the shadow mailbox.
- A range of extensions to use for list mailboxes. You do not need these to set up ELA but you need them to provide extensions for the list mailboxes when you begin creating lists.

Workflow for implementing ELA

About this task

To administer the ELA and make it fully functional for the system, you must perform the following tasks:

Procedure

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

Creating a shadow mailbox

About this task

ELA distributes messages through a shadow mailbox. A properly-configured shadow mailbox helps the system block recipients from replying to ELA senders or distribution lists.

Procedure

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

Next steps

Configure this shadow mailbox on the System Mailboxes page.

Configuring a shadow mailbox

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **System Mailboxes**.
2. Enter the appropriate information required to configure a shadow mailbox.

For more information, see System Mailboxes field descriptions on page 111.

3. Click **Save**.

System Mailboxes field descriptions

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

Name	Description
System Mailboxes	
Internet Postmaster Mailbox Number	The mailbox number that users dial to access their Messaging mailbox.
Enhanced-List Application Shadow Mailbox Number	The mailbox number for the ELA shadow mailbox. Messaging uses the shadow mailbox and the Community ID settings to control the sending privileges of users who address messages to ELA lists.
System Attributes	
Maximum Administered Remotes	The maximum number of remote users that Messaging can accommodate.
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 page.
Miscellaneous Field Names	
Miscellaneous 1 Field Name **Miscellaneous 2 Field Name** **Miscellaneous 3 Field Name** **Miscellaneous 4 Field Name**	Do not use these fields. They will be discontinued in a future release.

Adding a new ELA list

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **Enhanced List Management**.
2. On the Manage Enhanced-Lists page, click **Create a New List**.

3. On the Create a New Enhanced-List page, enter appropriate information in the fields.

   For more information, see . on page 112.

4. Click **Save**.

Next steps

Reload the User List and Global Address List. For more information, see Loading lists on page 114.

Configure the External Hosts and Mail Options with the **Alias** field blank. For more information, see Changing external SMTP hosts on page 83 and Configuring Mail Options on page 205.

Create a New Enhanced-List field descriptions

Name	Description
BASIC INFORMATION *(Required Fields)	
***List Name**	The name of the list, up to 29 alphanumeric characters. You can also record a spoken name for the list by logging in to the mailbox from the telephone user interface (TUI).
***Password**	The password for the Enhanced-List mailbox, from 5 to 15 numeric characters. When you are modifying an existing Enhanced-List, leave this field blank to retain the existing password. Users only need to enter this password when they use the TUI or an e-mail client to log in to the Enhanced-List mailbox. You do not need to enter a password to send messages to the list.
***Mailbox Number**	A 3- to 10-digit mailbox number. ELA automatically creates a mailbox with this mailbox number if one does not already exist. If a mailbox with the specified number already exists, ELA converts the existing mailbox into a list mailbox. The mailbox number must be: • Within the range of numbers assigned to your system. • Not be assigned to another local subscriber. • A valid length on the local machine. On a multisite system, the user mailbox can be of any length between 2 to 50 digits, the same would be

Name	Description
	validated 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, but the length of the numeric address must be at least one digit different than the length of the mailbox number. For example, if a mailbox number of 5671234 is in area code 222, the numeric address could be 2225671234.
PBX Extension	The primary telephone extension of the user. This is the number the telephony server calls for an internal call. On many systems, the PBX Extension is the same as the Mailbox Number.
***Class of Service (COS)**	The Class of Service for ELA is *8–ELA*.
***Community ID**	Do not change this field. The Community ID allows or denies voice mail among different communities.
ENHANCED-LIST FEATURES	
Permit Reply to Sender?	Specifies whether recipients are allowed to send replies to the originator of a message from an Enhanced-List. The default is *yes*.
Broadcast to All Local Subscribers?	The only option, *off*, sends ELA messages only to the list members you specify on the Manage Enhanced-List page. The system sends all broadcast messages as priority messages. Unheard broadcast messages do not take up space in a recipient's mailbox.
SUBSCRIBER DIRECTORY	
Email Handle	The e-mail handle for the list. Messaging automatically populates this field when you add a new list but you may change it. Do not enter the machine name and domain into this field. That information is automatically added when a user sends or receives e-mail. The default is <*ListName*>. For example: *AcctDept* .
Telephone Number	The telephone number for the list as it should display in address book listings, such as for e-mail client applications. The entry does not have a specified format, but all entries should be formatted consistently. The entry may be up to 50 characters long and may contain any combination of digits, period, hyphen, plus sign, and parentheses; that is 0-9 . - + ( ) .

Name	Description
Common Name	The common name for the list. Messaging automatically populates this field when you add a new list but you may change it. The Common Name displays in address book listings, such as for e-mail client applications. The default entry is the same as the ListName.
ASCII Version of Name	If the list name is in multi-byte character format, type its ASCII translation.
SUBSCRIBER SECURITY	
Immediately Expire Password?	Allows you to forcibly expire the mailbox password if you have a security situation such as a change in mailbox ownership. The default is *no*.
Is Mailbox Locked?	A user may complain that the mailbox is suddenly inaccessible (locked), possibly because of too many unsuccessful attempts to login. In some situations, you may want to add an extra layer of protection by selecting yes to lock the mailbox and prevent access to it.
MISCELLANEOUS	
Miscellaneous1 **Miscellaneous2** **Miscellaneous3** **Miscellaneous4**	Do not use these fields. They will be discontinued in a future release.

Loading lists

About this task

Use the System Operations page to load the following lists:

- User List
- Global Address List

Procedure

1. On the Administration menu, click **Messaging** > **Advanced** > **System Operations**.
2. Under **Reload Caches**, click **Reload** for the appropriate list.

Administering an ELA List

About this task

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

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **Enhanced List Management**.
2. On the Manage Enhanced-Lists page, you can click on buttons to:
   - Sort the lists.
   - Display a report of all the lists.
   - Create a new list. See Adding a new ELA list on page 111.
   - Select a list and then open it 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 e-mail addresses. If you type in a last name which 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 its attributes.

   An ELA list can contain nested ELA lists.
3. Click **Save**.

Sort Enhanced-List field descriptions

Make selections in the following rows to determine the display order of the Manage Enhanced-Lists display or Report:

Name	Description
Sort Keys	Determines the order in which the Manage Enhanced-Lists 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 there are ties in the primary sort.
Sort Order	The order in which lists are displayed. • *ascending* order (a-z, 0-9) • *descending* order (z-a, 9-0)
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 Class-of-Service number of each enhanced list.
Community ID	The community to which each enhanced list is assigned

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.

Name	Description
Reply?	Whether recipients of messages that ELA distributes can reply to enhanced-list messages.
Broadcast?	Whether messages sent to this list are also broadcast to all local subscribers.
COS	The Class-of-Service number of each enhanced list.
CID	The community to which each enhanced list is assigned.

Chapter 10: Caller applications

Caller applications overview

Caller applications enhance the Telephone User Interface (TUI) with custom menus and prompts that guide callers to the appropriate recipient. One caller application contains all custom menus and prompts associated with a unique mailbox.

When you create a caller application, you associate it with a site. The storage server for that site deploys the caller application to each application server in its 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, they are backed up each time you back up the message store.

Caller Applications Editor

Caller Applications Editor

Use the Caller Applications Editor to create custom menus and to configure caller application properties. In the Messaging environment, caller applications accomplish most of the same functions as Automated Attendants. The Caller Applications Editor runs as a plug-in within the Microsoft Management Console (MMC). You can access information about MMC through its Help menu.

System requirements

To use the Caller Applications Editor, you need:

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

- Microsoft Management Console (MMC 3.0)
- .NET 3.5

• Administrative permissions on the computer.

Containers

A Microsoft Management Console (MMC) container allows you to group related items. MMC displays containers as folders in the navigation pane of the Caller Application Editor. For more information about containers, see the MMC Help.

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

• 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 the Auto Attendant

• Time zone of the application server (not the storage server, if different)

• The caller menu logic

For more information, see:

• Worksheet for container properties on page 126.

• New Caller Application field descriptions on page 133.

Prompts

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

• Prerecorded audio prompts in .wav format

• Text-to-Speech prompts

Recording an audio prompt

Procedure

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

Text-to-Speech prompts

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

Unsupported characters	Encoded characters
<	&lt;
>	&gt;
&	&amp;
'	&apos;
“	&quot

Menus

Caller application menus are based on dual-tone multi-frequency (DTMF) key entries that route calls to a unique mailbox. You use the 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 options
- Up to 10 DTMF key entries that act upon the menu options defined by the Instruction prompt.

Menu flexibility

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

A Business Hours menu typically has a robust set of prompts and DTMF key entries. An Off Hours menu is typically much simpler, and may only include an On Answer prompt that explains that a business is closed. However, the 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 select the type of action that you want each key press to perform. These actions are:

Action	Description
Auto Attendant	Forwards the call to the Auto Attendant so the caller can dial-by-name or dial-by-extension.
Go to mailbox number	Routes the call to a specified voice messaging mailbox. For example, a non-business hours mailbox or an information-only mailbox.
Subscriber login	Routes the call to the voice messaging pilot extension so users can log in to their 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 may use this as a “Next” action.
Hang up	Ends the call.
Transfer to extension	The call transfers to another extension. For example: • Transfer to a specified extension. For example, Customer Service. • When a user forwards calls to a caller-application extension. For example, if an employee changes internal extensions or if a previously used extension is out of service.
Not active	The default for all DTMF keys before you assign an action. Unused keys should 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 prompt finishes playing, 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 option	**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.
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.*	Not applicable

	Change action or select the prompt dialog	
Menu option	**First perform this action:**	**Then perform this action:**
Key 1	**Play prompt** Use Text to Speech to say: *The ABC store is open from 10 am to 7 pm, Tuesday through Saturday.*	**Continue menu** 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** Caller can press another key or hang up.
Key 3	**Auto Attendant** The call is routed to the auto attendant so the caller can enter an extension.	Not applicable
Key 4	**Auto Attendant** The call is routed to the auto attendant so the caller can enter an extension.	Not applicable
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 call is put into this mailbox.	Not applicable
Key 6	**Transfer to extension** Then enter the extension of customer service. The call is blind transferred to this extension.	Not applicable
Key 7	**Subscriber login** Transfer the call to the voice messaging pilot number so the user can log in to their mailbox. (This option is not listed in the Instructions because it is only for employees.)	Not applicable
Key 8	**Hangup** End the call.	Not applicable
Key 9	**Not active**	Not applicable
Key 0	**Not active**	Not applicable

Schedules

Business schedules

The business schedule defines the operating hours for your organization.

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

The default business hours are 8:00 AM through 5:00 PM, Monday through Friday. However, you can change these hours in the 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 this predefined holiday schedule.
- When you create a new holiday schedule, give it a unique descriptive name. For example, *2010 Corporate Calendar*.
- The holiday menu plays for the entire day specified by the holiday schedule. This 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 it. Allow a few seconds for the update to complete.

Planning a caller application

Caller applications checklist

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

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

No.	Task	References	✔
1	Create a plan for the caller menus and prompts.	• Worksheet for container properties on page 126 • Worksheet for menus on page 127	
2	Define a location on the storage server for storing mailboxes associated with caller applications.	Creating containers on page 133	
3	Define a caller application container.	Creating containers on page 133	
4	Define the schedule for each caller menu.	• Creating business schedules on page 135 • Creating holiday schedules on page 136	
5	Create the call menus.	Creating menus on page 135	
6	Load audio prompts	Assigning audio prompts to menus on page 136	

Worksheet for container properties

Tip:

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

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

Worksheet for menus

Use this worksheet to plan the logic for a Business Hours or Off Hours menu. See Example menu on page 123 for an example of a Business Hours menu.

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

		Complete only for Play Prompt actions	
Prompt or key press	**Menu action (select one)**	**Filename or TTS text**	**Define next action**
	• Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 1	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 2	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 3	• Play Prompt • Auto Attendant • Go to mailbox number: _____		

		Complete only for Play Prompt actions	
Prompt or key press	**Menu action (select one)**	**Filename or TTS text**	**Define next action**
	• Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 4	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 5	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 6	• Play Prompt • Auto Attendant • Go to mailbox number: _____		

		Complete only for Play Prompt actions	
Prompt or key press	**Menu action (select one)**	**Filename or TTS text**	**Define next action**
	• Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 7	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 8	• Play Prompt • Auto Attendant • Go to mailbox number: _____ • Subscriber login • Transfer to Caller Application: _____ • Hangup • Transfer to extension: _____ • Not active (default)		
Key 9	• Play Prompt • Auto Attendant • Go to mailbox number: _____		

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

Installing the Caller Applications Editor

Procedure

1. Open your browser and navigate to `http://<Messaging server>/download/CallerApplicationsEditor.msi`.

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

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

Changing the Caller Applications password

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

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **System Policies**.
2. On the System Policies page under the Caller Applications Administrator heading, enter the new password in the **Password** field.
3. Enter the password again in the **Confirm password** field.

   For more information, see System Policies field descriptions on page 91.
4. Click **OK**.

Working in the Caller Applications Editor

Logging in to the Caller Applications Editor

Before you begin

- All prerequisite software is loaded on to your computer. See System requirements on page 119.
- You know the IP address or DNS name of the storage server.
- You know the password for the Caller Application Editor. When you access the software for the first time, the password is `caadmin01`.

Procedure

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

Result

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

Creating containers

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

Before you begin

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

Procedure

1. In the Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. Right-click **Caller Applications**.
3. Select **New** > **Caller Applications**.
4. If you are creating the first caller application for the system, identify the location for storing caller application mailboxes.

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

   For more information, see New Caller Application field descriptions on page 133.
6. Click **OK**.

Next steps

Go to Creating menus on page 135.

New Caller Application field descriptions

These fields define the caller application container.

Name	Description
Name	The name of the caller application.

Name	Description
Mailbox number	The mailbox number for the user account associated with the caller application. All mailbox numbers for user accounts must be unique. However, they do not have to match the extension.
Include in Auto Attendant Directory	Whether you want to make the caller application accessible through the Auto Attendant directory. If you do, complete the **Pronounceable name** field if the name might be pronounced several ways.
Extension	The extension that callers dial to reach the caller application. The extension must be unique.
Additional extensions	Any additional extensions that you want to associate with the caller application. Examples of when to enter additional extensions are: • When multiple DID numbers access the caller application. • When 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.
Pronounceable name	If a user or info mailbox has a name that might be pronounced several ways, spell the name the way you would pronounce it. For example, spell Dan DuBois Dan Doobwah. This entry may reduce the number of attempts it takes the Speech Recognition feature to match a spoken name to the name in the Auto Attendant directory. You can also enter an alternative name. For example, if the original name for the caller application is *Customer Support*, you might enter *Technical Support* in this field. The speech engine will recognize both spoken names.

Creating menus

Before you begin

You have created a container for the caller application. See Creating containers on page 133.

Procedure

1. In the Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. In the Name pane, right-click on 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.
5. Repeat Step 3 and Step 4 for each additional menu.
6. If you are using audio prompts, go to Assigning audio prompts to menus on page 136.
7. Click **OK**.

Creating business schedules

Procedure

1. In the Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. In the Name pane, right-click on 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 the year for which they are created. For example, if you create a holiday schedule for Christmas day 2011, you must create a new schedule for Christmas day 2012.

Procedure

1. In the Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. Right-click **Holiday Schedules**.
3. Select **New** > **Holiday schedule**.
   MMC adds a New Holiday Schedule container.
4. Right-click on the **New Holiday Schedules** container.
5. Select **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**.
10. 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 the Caller Applications Editor, expand the **Caller Applications Editor** folder.
2. In the Name pane, right-click on the caller application and then select **Properties**.
3. Select the **Prompts** tab and then click **Add**.

4. Navigate to the folder that contains the prerecorded audio prompts.
5. Select a .wav file.
   You can select multiple files at the same time.
6. Click **OK** to add the files to the caller application.
   The caller application that you selected can use the prompts for any Play Prompt action. See Menu actions on page 122.
7. Repeat these steps for each additional caller application.

Deploying a caller application

Before you begin

You have created and tested the caller application.

Procedure

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

Result

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

Chapter 11: Managing software

Viewing currently installed software

Use this procedure to view a list of software packages that are currently installed on the Messaging server. You may want to 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 packages installed properly)

Procedure

On the Administration menu, click **Messaging** > **Software Management** > **List Messaging Software**.

The page displays the packages that have been installed in priority order. You can change the view by selecting:

- **Display software in alphabetical order**
- **Display software installation time**

Applying software updates

Downloading remote field updates

Before you begin

You need a login and entitlement to download Avaya software packages.

Procedure

1. From any computer, navigate to the Avaya Support Web site.
2. In the navigation pane, click **Downloads**.
3. Begin entering the word `messaging`.

   After you enter the first few letters, the system displays a list of messaging products.
4. Select Avaya Aura® Messaging.
   The Support site displays a list of download packages.
5. Select the package that you want to download.

   The Support site displays the Release Notes for the package. Read this information to ensure that you have selected the appropriate package.
6. Click the **Download** tab to view the available downloads.
7. Click the **login** link and enter your login information.

   You can sign up for a login on the Login Now page.
8. Download the file(s).

Next steps

Copy the files to each Messaging server in your configuration.

Copying files to the server

Use the System Management Interface (SMI) to copy the latest RFUs and optional languages to the Messaging server.

Procedure

1. Log on to the SMI. For more information, see Logging in to Messaging on page 16.
2. On the Administration menu, click **Server (Maintenance)** > **Miscellaneous** > **Download Files**.
3. Select one of the following:
   - **File(s) to download from the machine I'm using to connect to the server**.
   - **File(s) to download from the LAN using URLs**.
4. Enter the name of the proxy server, if required. If a proxy server is required for an external Web server (not on the corporate network), entered it in a `server:port` format. Consult your network administrator, if needed.

5. Click **Browse** to locate the file(s).
6. Click **Download** to copy the files to the Messaging server.
   The Download Files Results page displays a list of downloaded files.
7. Repeat Step 3 through Step 6 until you have downloaded all required RFUs.

Next steps

Install the downloaded RFU.

Installing an RFU

Before you begin

You have downloaded the remote field update (RFU) files and copied them on to each Messaging server in your configuration.

About this task

Important:

Messaging stops all processes during an RFU installation. Do not start Messaging during the installation. Start Messaging after you have installed the RFU. See Starting Messaging on page 21.

Procedure

1. Log on to the System Management Interface as a privileged administrator.
   See Logging in to Messaging on page 16.
2. On the Administration menu, click **Messaging** > **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.
   The Following packages will be installed... page displays the Messaging RFUs.
4. Click **Install selected packages**.
   If the RFU made modifications to the SMI pages, you may be prompted to close and reopen this page. Follow any instructions that appear during this process.
5. Verify that the RFU was installed. See Viewing currently installed software on page 139.
6. Repeat this procedure on *each* Messaging server in your configuration.

Installing software

The software installation page displays the packages available for installation.

Procedure

1. Perform a full system backup. See Backing up the system files now on page 147.
2. On the Administration menu, click **Messaging** > **Software Management** > **Software Install**.
3. Click **Continue without current system backup**.

   The system lists the all of the available software packages that you can install, including all software packages and patches that you have previously downloaded. For more information, see Copying files to the server on page 140.
4. Select the software package(s) that you want to install.
5. Click **Install selected packages**.

Verifying system installation

About this task

The Verify System Installation page confirms that:

- The primary software packages for the system are properly installed
- A complete version of each application-specific package exists on the system

The system takes a few minutes to perform a series of background checks on the system software. The system checks the content of each installed executable or help file, but not data files, to verify that they were unchanged during the lifetime of the system.

Procedure

On the Administration menu, click **Messaging** > **Software Management** > **Software Verification**.

Result

The Verify System Installation page displays each of the primary software packages and protocols installed on the system and notes any exceptions.

Installing advanced software

About this task

Use these instructions to install required software such as remote field updates (RFUs). Most software installations require that the voice system is not running. So plan to install the software that you download during low usage hours.

You can also install additional software packages from a CD inserted into your laptop or from technical support Web sites.

Note:

Do not install advanced software unless you are specifically instructed to do so by Avaya services.

Procedure

1. On the Administration menu, click **Messaging** > **Software Management** > **Advanced Software Install**.
2. Click **Continue without current system backup**.

   The system lists the all of the available software packages that you can install, including all software packages and patches that you have previously downloaded. For more information, see Copying files to the server on page 140.
3. Select the software package(s) that you want to install.
4. Click **Install selected packages**.

Removing software packages

Procedure

1. On the Administration menu, click **Messaging** > **Software Management** > **Software Removal**.
2. Select the software packages to be removed.
3. Click **Submit**.
   The system removes the software.

Chapter 12: Back up and restore

Overview of backup and restore

Purpose of Backup and Restore

The Messaging server backs up Messaging data over the customer's LAN to an external ftp server. This data can be backed up at the same time as the server data, or independently. In the event of a system failure, the information stored on the external server is used to restore the system to an operational state. Messaging supports up to 20000 mailboxes. Back up of the Messaging data could easily reach 50 Gigabytes or more. It is unusual for customers to support transfers of single files of this size. Hence, Messaging data backup consists of multiple files, each small enough to be transferred in a customer’s environment. Supported backup methods are:

- FTP
- SFTP
- SCP

The system administrator who is administering network backups using FTP, SCP, or SFTP needs to be cognizant of the possible file storage size and any limitation of the storage size on the customer’s data network.

A system administrator can mitigate the backup file size by:

- Limiting the mailbox size of users to fewer hours of storage, so that users do not have more than 10 or so minutes of voice storage in their mailbox
- Limiting the number of days a message can remain in a mailbox before the message is deleted. Currently the system defaults to 45 days of shelf life for a message before it is deleted. The system automatically deletes messages with the nightly audits when the messages age to the administered number of days.

Data that you can back up and restore

You can back up any combination of the four messaging data types at any time manually (Backup Now) or according to a schedule automatically (Scheduled Backup). The four data types are:

- Translations
- Announcements
- Messaging names
- Messaging greetings and messages

Translations

Translations comprise system administration data:

- Detailed system data on shared memory, speech file system pointers, and so on
- Alarm management information
- A list of enabled features
- A list of installed software
- Messaging digital networking connectivity and communication information
- Message headers, mailing lists, user profiles (including automated attendant administration), and message-waiting indicator status
- Switch integration parameters
- Hard disk configuration

In addition to the scheduled backups, you can also perform a backup now whenever you make extensive changes to user profiles.

Announcements

Announcements are prompts and phrases that guide a user through the Messaging application. This data type does not require a backup unless the system has customized announcements that have been changed recently. If customized announcements are not being used, a backup of announcements exists on the Avaya support site. See https://support.avaya.com.

Messaging names

The messaging names data type contains recorded user names. You must perform a backup now of this data type after additional user names have been recorded.

Voice messages

Voice messages are recorded messages that users have received and retained. This includes the primary voice greeting, multiple personal greetings, and automated attendant menus and messages.

FTP server availability

If the FTP server is not available at the time of backup, the backup fails. You must ensure that maintenance on the FTP server does not coincide with backup timings. A backup requires 30 to 40 minutes, or even more, depending on the size of your files and the network traffic.

About restoring backed-up system files

Messaging information stored on a server during data backups is used to restore the system to an operational state. Use the **View/Restore Data** page to restore backed-up system files.

You are likely to restore backups when directed to do so by an alarm repair action.

Backup Verification

Avaya recommends that you verify the success of each backup you run. A backup can include a variety of data types, in addition to Messaging server data. The View Backup Log screen,

available from the Server (Maintenance) Web page, displays all backed up files. You can open any file and view the data types that it contains.

Note:

There is no partial success of a backup. A Messaging backup is successful only if it includes all the data that you selected for backup.

Backing up the system files now

You can manually backup your system at any time or you can schedule routine backups. A backup that you perform manually is often called an attended backup. Use the following instructions to perform attended backups.

Procedure

1. Stop Messaging. See Stopping Messaging on page 20.
2. On the Administration menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Backup Now**.

   The system displays the **Backup Now** page.
3. Under the **Data Sets** heading, select **Specify Data Sets**. Then select:
   - **Server and System Files**
   - **Security File**
   - **Messaging**
4. Under **Messaging**, select: **Messaging Translations, Names, and Messages**.
5. Under the **Backup Method** heading, select **Network Device** and then complete the following fields:
   a. **Method**
   b. **User Name**
   c. **Password**
   d. **Host Name**
   e. **Directory**
6. Under the **Encryption** heading, select **Encrypt backup using pass phrase** and then enter a phrase.
7. Under the **Download Size** heading, enter a value from 1 through 200 to limit the size of a transferable file over the network and ensure a successful backup of the Messaging data.

Ensure that the number you enter is less than or equal to the maximum size that the network allows for transferring files. The system creates a backup image that may have more than one file. No files will exceed the size that you specify.

8. Click **Start Backup**.
   For more information, see Backup Now field descriptions on page 148.

Backup Now field descriptions

Settings	Description
Data Sets	Indicates the data sets to be backed up. Available options are: • **Server and System Files**: Back up the variable information to configure the server for a particular installation. • **Security File**: Back up the variable information to maintain security for the server. • **Messaging** Back up one of the following Messaging options: - **Messaging Announcements** - **Messaging Application, Translations and Messages** - **Messaging Application, Translations, Names, and Messages** - **Messaging Application, Translations and Names** - **Messaging Application and Translations** - **Messaging Application** - **Messaging Translations and Messages** - **Messaging Translations, Names, and Messages** - **Messaging Translations and Names** - **Messaging Translations**

Settings	Description
Full Backup	The full backup includes security data sets and files that configure both the Linux operating system and the applications. A **Full Backup** does not include any of the Messaging Data Sets.
Backup Method	Following are the three methods available for backup: • **SCP**: A means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol. • **FTP**: To back up data to an FTP server. When you choose this selection, you must also enter a user name, password, host name, and directory. The default directory for backup data on the FTP server is /var/home/ftp. If you want to use the default directory, enter a forward slash (/) in the directory field. You must start the FTP server before backing up. To enable the FTP server, see FTP Server. • **SFTP**: A network protocol that provides file transfer over data streams. The SFTP client is added to all Linux platforms
Encryption	Defines if the backup data is to be encrypted. 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, back slash, single back quote, quote, percent sign).
Download Size	Indicates the maximum file transfer size in the Download size for the data being transferred box. This ensures the backup of large data (such as the backups that contain messages) over the networks that limit the size of a transferable file, The maximum size of an individual backup file is the value specified in the Download size for the data being transferred box multiplied by 100 MB. Valid values range from 1 to 200, indicating 100 MB to 20 GB. The default value is 5 (500 MB). The specified value in the Download size for the data being transferred box should be less than or equal

Settings	Description
	to the maximum file transfer size allowed on the network.

Scheduled backups

About scheduled backups

Use Backup Now when you want to back up system data immediately. For example, you may want to back up data very soon after you have installed the Messaging server and/or the messaging system. Additionally, you may want to run the backup procedure just before making a change to your system. Doing so ensures that the most recent data is backed up, including data that is new since the last scheduled backup was run.

Additionally, the messaging backup files can be quite large. As a result, your LAN network connection may fail during the backup. In this case, you can run a scheduled backup instead, which allows the Messaging server to handle breaks in the LAN connection and ultimately create a successful backup. To run a scheduled backup in case of a failed backup now, you can simply set the schedule to run on the current day and 5 or 10 minutes in the future. See Create (add) a new backup schedule on page 150.

Adding a new backup schedule

About this task

To create a backup schedule, you first decide what type of data you want to back up. You 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** > **Schdeule Backup**.

   The system displays the **Schedule Backup** page.

   If backups are already scheduled, the screen lists the current backup schedules. Look at it carefully to determine what backup schedule you want to add.

   If this is the first backup schedule to be created, the Schedule Backup screen displays a message that there is no record of any backup schedule.

2. Click **Add**.

   The system displays the **Add New Schedule** page.

3. Select **Specify Data Sets**.

4. Select **Messaging**.

5. Select **Translations, Names, and Messages**.
6. Select a **Backup Method**.
   a. Enter **User Name**.
   b. Enter **Password**.
   c. Enter **Host Name**.
   d. Enter **Directory**.
7. Set a password to encrypt the backup data.

   Avaya recommends that you encrypt the backup data. You must remember the pass phrase because you cannot restore the data without it.
8. Enter a value from 1 through 200 to limit the size of a transferable file over the network to ensure a successful backup of the Messaging data.

   The specified value in the Download size field for the Messaging data being transferred must be less than or equal to the maximum file transfer size allowed on the network. The resulting backup image comprises of one or more files that do not exceed the specified size. For example, if you set the value as 5, the size of the data is 500 MB.
9. If you want to encrypt the backup data, click the box in the Encryption area of the screen and enter a pass phrase using an arbitrary string of 15 to 256 characters.
10. If necessary, scroll to the bottom of the screen and 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** drop-down.

    You can select multiple days but only one time for the backup schedule to run.
11. Click the **Add New Schedule** button to save the schedule you just created.

    The system displays the **Schedule Backup** page with the new backup schedule added to schedule list.

Modifying a backup schedule

Procedure

1. On the Administration menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Schdeule Backup**.

   The system displays the **Schedule Backup screen**.

   If backups are already scheduled, the screen lists the current backup schedules. Look at it carefully to determine what backup schedule you want to add.

If this is the first backup schedule to be created, the Schedule Backup screen displays a message that there is no record of any backup schedule.

2. From the list containing the current scheduled backups, select the backup schedule you want to modify.

   The Change Current Schedule page appears.

3. Modify information as appropriate.
4. Click **Change Schedule**.

Removing a backup schedule

Procedure

1. On the Administration menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Schdeule Backup**.

   The system displays the **Schedule Backup screen**.

   If backups are already scheduled, the screen lists the current backup schedules. Look at it carefully to determine what backup schedule you want to add.

   If this is the first backup schedule to be created, the Schedule Backup screen displays a message that there is no record of any backup schedule.

2. From the list containing the current scheduled backups, select the backup schedule you want to delete.
3. Click **Remove**.

   The schedule backup list gets updated.

Viewing backup history

Procedure

1. On the Administration menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Backup History**.

   The Backup History page appears 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 Backup History Results page appears with the details of the selected backup.

Viewing backup logs

When you back up data, the system creates an image as a tar file that contains information, such as what data sets were backed up, whether or not the backup was successful, and how the data was recorded. Use the Backup Logs to verify the success or failure of the of a backup.

About this task

To verify a backup:

Procedure

1. On the Administration menu, click **Server (Maintenance)** > **Data Backup/Restore/** > **Backup Logs**.
2. On the Backup Logs page, look through the log until you see a backup image you want to preview or restore. Select the log by clicking the radio button to the left of the image.

   If no entries exist in the backup log, you will see a message that there is no record of any backups.
3. Click **View**.

   The View/Restore Data Results page appears.
4. Enter the **Username** and **Password** for file transfer settings.
5. Click **Preview**.

Performing a restore

About this task

Note:

You must stop your messaging system before you restore data. See the instructions that follow.

The time required for a restore depends on the amount of data on the system and the speed of LAN traffic. The following procedure works for both attended and unattended backups.

Procedure

1. Stop the messaging software (voice system).
2. On the Administration menu, click **Server (Maintenance)** > **Data Backup/ Restore** > **View/Restore Data**.

   The **View/Restore Data** page appears.
3. Under the **View current backup contents** in heading, select **Network Device**. Then use the same information that you used when you backed up the data to complete the following fields:

   a. **Method**

   b. **User Name**

   c. **Password**

   d. **Host Name**
4. Click **View**.

   The View/Restore Data results page lists the backup images stored in the location you specified. The most recent backups are listed at the bottom of the list.

   You must select a backup image before you click View, or an error message appears. To clear it, simply click the browser's Back button, then select a backup image.
5. Select the backup image you want to view or restore by clicking the corresponding radio button.

   If you must restore the Messaging server data sets as well as the messaging data sets, you restore the Messaging server data first. If the hard drive is new, and the release number of the software on the hard drive is more recent than that of the backup data, click **Force restore if backup version mismatch** and Force Restore if server name mismatch.
6. Click one of the following buttons:

   • Preview. Use the Preview button if you are not sure you have selected the correct backup image. When you click Preview:

   - A **View/Restore Data Results** screen displays a brief description of the data associated with the backup image.
   - Messaging data will have one of the following names attached to the backup file name:

     • audix-ann for announcements

     • audix-tr-msg for translations and messages

     • audix-tr-name-msg for translations, names, and messages

     • audix-tr-name for translations and names

     • audix-tr for translations only

- You can then click **Restore** on this second screen to begin the restore process. If the hard drive is new, and the release number of the software on the hard drive is more recent than that of the backup data, click on **Force restore if backup version mismatch** and Force Restore if server name mismatch.

- Restore. When you click **Restore**, the system displays a View/Restore Data results screen that tells you whether or not the restore procedure is successful.

7. Do one of the following:
   - If you do not have any remote networked machines, continue with step 8.
   - If you have any remote networked machines, do the following:

   a. Logoff of the Messaging server.
   b. Log in to the Messaging Web page.
   c. Run a manual update to and from all remote networked machines to correct any database inconsistencies.

      See Running a Remote Update Manually.
   d. Continue with step 8.
8. Restart the Messaging software.

Viewing restore history

The Restore History page displays the 15 most recent restores which are identified by the server name, date, and time of the backup and the process ID.

About this task

Procedure

1. On the Administration menu, click **Server (Maintenance)** > **Data Backup/Restore** > **Restore History**.

   The Restore History page appears with a list of the 15 most recent restores.
2. To check the status of a specific restore, select the restore and click **Check Status**.

Chapter 13: Alarms

Alarms

System errors are recorded in the Maintenance log. The Messaging system attempts to diagnose and isolate these errors from the system and sends an alarm to the alarm log if it cannot correct the error automatically. The system also sends alarms to the Messaging server Alarm log.

The contents in the messaging alarm log represent all the significant problems the system detects. Therefore, the Alarm Log is a good starting point for troubleshooting the system. However, you might also wish to use the Server Alarm Log that lists all alarms on the Messaging server, including messaging alarms. This log is available on the **Server (Maintenance)** Web page through the option Current Alarms. For details, see the maintenance documentation on Messaging that can be downloaded from Avaya Support Site.

The Messaging alarm log contains two types of entries:

- Active alarms

  An active alarm indicates a current problem in the system.

- Resolved alarms

  Resolved alarms have been corrected either automatically or through a repair procedure.

Three alarm levels indicate the severity of an alarm:

Major Alarms	Major 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, a major alarm is generated. Major alarms are repairable by technicians.
Minor Alarms	Minor alarms indicate problems that could affect full service but are not critical to system operation. For example, if a network connection occurs, a minor alarm is generated. Minor alarms are repairable by technicians.
Warning alarms	Warning alarms indicate problems that could potentially affect system service if not resolved. For example, if the customer system administrator does not create a trusted server password and a trusted server tries to log in, a warning alarm is generated. Warning alarms are repairable by the customer.

When an active alarm is corrected, its 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 a remote service center.

Alarm Notification

Viewing the administrator's log and the alarm log on a daily basis, either from the messaging administration screens or from the alarm log on the Messaging server, is the best way to be informed of new entries. Active alarms (alarms that have not been resolved) and new entries to the administrator's log are noted on the STATUS line.

Important:

The STATUS line can display multiple levels of alarms. The alarm level is important because it 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 between the responsibility of the system administrator (warning alarms) and the responsibility of the remote service center (major and minor alarms).

Alarms and notifications

The Application Server, Storage Server, and AxC generate system alarms and error logs that you can gain access to by using the System Management Interface.

Notifications generated by alarms can be sent to any one of the following recipients:

- Avaya Services
- A customer through a Network Management Station (NMS)
- Avaya Partners

  Note:

  Avaya Partners need 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 the alarm notifications to a service organization:

- SAL

  SAL is an Avaya 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 is a software package that facilitates remote access to support personnel and tools that need to access supported devices. The SAL Gateway is installed on a Red Hat Enterprise Linux host in the customer network and acts as an agent on behalf of several managed elements. The Application Server sends the alarms to a SAL Gateway server. The SAL Gateway server is configured to forward the alarms to various NMS destinations. A SAL Gateway is also included in CDOM on the server that runs Messaging.

- SNMP

  The Application Server and Storage Server can also use SNMP to send the alarm notifications to a customer NMS. The Storage Server provides support for SNMP GET requests. The Application Server does not provide support for SNMP GET requests. Neither the Application Server nor the Storage Server provides support for SNMP SET requests.

Viewing current alarms

The Current Alarms Web page provides a list of alarms and their origin.

About this task

To view current alarms against the messaging software:

Procedure

1. On the Administration menu, click **Server (Maintenance)** > **Alarms** > **Current Alarms**.
2. Check if any alarms are present under the **Messaging Alarms** heading.

Current Alarms field descriptions

Field Name	Description
Product ID	Product ID is a number that uniquely identifies the server.
Messaging Product ID	Messaging Product ID is a number the uniquely identifies the Messaging Product.

Field Name	Description
ID:	ID is the unique identification number assigned to the alarm.
APP	Name of the application.
Source	Is the abbreviated name of the software module that generated the alarm, as follows: • **ABR**: Arbiter • **ENV**: Environment • **FSY**: File synchronization • **GAM**: Global alarm manager • **GMM**: Global maintenance manager • **KRN**: Kernel • **LIC**: License server • **logon**: Logon attempts • **NIC**: Ethernet network interface • **SME**: Server maintenance engine • **SVC_MON**: Service monitor • **TLG**: Trace log • **UPS**: Uninterruptible power supply • **USB**: Universal serial bus • **VFM**: Virtual fabric manager • **_LX** : Linux • **_TM**: Translation manager • **_WD**: Watchdog
EvtID	Is the event identification number for each alarm, which is used to identify a particular event from a given source that generated the alarm.
Lvl	Indicates the level of the alarm (minor, major, or warning).
Ack	Displays a Y (yes) or N (no) to indicate whether or not the alarm has been acknowledged by the Initialization and Administration System (INADS).
Location	Location where the alarm originated.
Date	Is the time stamp assigned to the alarm when it originated.

Configuring SNMP trap destinations

Use the SNMP Traps page to configure destinations for SNMP traps or informs (alarms and notable events) on the corporate network. Some form of corporate network management system (NMS) must be in place to collect the SNMP messages. In addition, the SNMP ports must be enabled on the Ethernet interface to the corporate LAN.

Note:

Prior to making any configuration changes the Master Agent must be put in a **Down** state. The Master Agent status is shown on the SNMP Trap page. Once the configuration has been completed, then the Master Agent must be placed in an **Up** state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages must be completed before starting the Master Agent. Please use the Agent Status page to start or stop the Master Agent. For more information, see Viewing and modifying agent status on page 170.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Server (Maintenance)** > **SNMP Traps**.
   The SNMP Traps page is displayed. The page displays existing **SNMP traps** and status of **Master Agent**.
2. Click **Add/Change**.
3. Enter appropriate information in the fields.
   For more information, see Configure SNMP trap destinations field descriptions on page 161.
4. Click **Submit**.

Configure SNMP trap destinations field descriptions

Field Name	Description
SNMP version	The three final fields on this page are blank if SNMP Version 1 or Version 2c are used.
Status	Shows if the configured destination is enabled or disabled. Traps or inform requests (informs) are only sent to a

Field Name	Description
	destination if enabled. Disabling a destination keeps the configuration data in the file, but stops traps and informs from being sent.
Notification	Refers to traps or inform requests as described above.
Community Name	The authentication mechanism used by the different SNMP versions. **Community Name Authentication** is a plain text string used for SNMP v1 and v2c.
User Name	User Name is part of the user-based security model for SNMP v3. This character string indicates the user who is authorized to send traps to the destination.
Authentication Password:	Pass phrase for the user specified in the User Name field, used to digitally "sign" v3 traps.
Privacy Password	Pass phrase for the user specified in the User Name field, used to encrypt v3 traps.

Changing an administered SNMP trap

Procedure

1. On the server's Server Administration Interface, click **SNMP Traps**.
2. Check the status of the Master Agent.

   The Master Agent must be in a "Down" state before you make changes to the SNMP Traps screen.

   - If the status of the Master Agent is "Up": Select Agent Status from the navigation bar and click **Stop Agent**. Once the Master Agent reaches a "Down" state, return to the SNMP Traps screen by clicking **SNMP Traps** on the navigation bar.
   - If the status of the Master Agent is "Down," continue with 3.
3. Under the Current Settings heading on the SNMP Traps screen, click the radio button associated with the trap that you wish to change.
4. Make the changes to the trap destination and click **Change**.
5. If you are finished changing the trap destinations, you must start the Master Agent.

To start the Master Agent, select Agent Status from the navigation bar and click **Start Agent**.

Deleting an administered SNMP trap

Procedure

1. On the server's Server Administration Interface, click **SNMP Traps**.
2. Check the status of the Master Agent.

   The Master Agent must be in a "Down" state before you make changes to the SNMP Traps screen.

   - If the status of the Master Agent is "Up": Select **Agent Status** from the navigation bar and click **Stop Agent**. Once the Master Agent reaches a "Down" state, return to the SNMP Traps screen by clicking **SNMP Traps** on the navigation bar.
   - If the status of the Master Agent is "Down," continue with 3.
3. Under the **Current Settings** heading on the SNMP Traps screen, click the radio button associated with the trap that you want to delete.
4. Click **Delete**.

   The SNMP Traps screen appears displaying the updated trap destination list.
5. If you are finished deleting the trap destinations, you must start the Master Agent.

   To start the Master Agent, select Agent Status from the navigation bar and click **Start Agent**.

SNMP filters administration

Use the SNMP Filters screen to perform the following tasks:

- Adding an SNMP filter
- Changing an SNMP filter
- Deleting one or all SNMP filters
- Customer Alarm Reporting Options

The filters are used only for Communication Manager and determine which alarms are sent as traps to the trap receiver(s) that are administered using the SNMP Traps page. For more information on how to administer an SNMP trap, see SNMP traps administration.

Important:

Filters created by Fault and Performance Manager (FMP) do not display on the SNMP Filters screen. If you are using FMP, create the filters using the FMP application. The FMP application provide some additional capabilities that are not available using the SNMP Filters screen.

Adding an SNMP filter

About this task

Use the following steps to add a filter.

Procedure

1. On the server's Server Administration Interface, click SNMP **Filters** under the Alarms heading.
2. Click **Add**.
3. **Severity**: Select from one or more of the following alarm severities that will be sent as a trap:
   - Active
   - Major
   - Minor
   - Warning
   - Resolved
4. **Category and MO-Type**: Select the alarm category for this filter from the drop-down menu.

   The **MO-Types** that display are based on the `Category` that you select. The available categories with their associated MO-Types are listed in the table on page 164.

   Table 1: Category with associated MO-Type table

Category	MO-Type
adm-conn	ADM-CONN
announce	ANN-PT, ANN-BD, ANNOUNCE

Category	MO-Type
atm	ATM-BCH, ATM-DCH, ATM-EI, ATM-INTF, ATM-NTWK, ATM PNC-DUP, ATM-SGRP, ATM-SYNC, ATM-TRK, ATM-WSP
bri/asai	ASAI-ADJ, ASAI-BD, ASAI-PT, ASAI-RES, ABRI-PORT, BRI-BD, BRI-PORT, BRI-SET, LGATE-AJ, LGATE-BD, LGATE-PT
cdr	CDR-LINK
data-mod	BRI-DAT, DAT-LINE, DT-LN-BD, PDMODULE, TDMODULE
detector	DTMR-PT, DETR-BD, GPTD-PT, TONE-BD
di	DI-BD, DI-PT
environ	AC-POWER, CABINET, CARR-POW, CD-POWER, EMG-XFER, EXT-DEV, POWER, RING-GEN
esm	ESM
exp-intf	AC-POWER, CARR-POWER, DC-POWER, EPN-SNTY, EXP-INTF, MAINT, SYNC, TDM-CLK, TONE-BD
ext-dev	CUST-ALM
generatr	START-3, SYNC, TDM-CLK, TONE-PT, TONE-BD
inads-link	INADS
infc	EXP-INTF
ip	MEDPRO, IPMEDPRO, MEDPORPT, H323-SGRP, H323-BCH, H323-STN, DIG-IP-STN, RDIG-STA, RANL-STA, NR-CONN, REM-FF, ASAI-IP, ADJLK-IP, SIP-SGRP
lic-file	NO-LIC, LIC-ERR
maint	MAINT
misc	CONFIG, ERR-LOG, MIS, PROC-SAN, SYSTEM, TIME-DAY
mmi	MMI-BD, MMI-LEV, MMI-PT, MMI-SYNC
mnt-test	M/T-ANL, M/T-BD, M/T-DIG, M/T-PT
modem	MODEM-BD, MODEM-PT
pkt	M/T-PKT, PKT-BUS
pms/jrnl	JNL-PRNT, PMS-LINK
pns	DS1C-BD, DS1-FAC, EXP-INTF, FIBER-LK, PNC-DUP, SN-CONF, SNC-BD, SNC-LINK, SNC-REF, SNI-BD, SNI-PEER
pncmaint	DS1C-BD, DS1-FAC, EXP-INTF, FIBER-LK, PNC-DUP, SN-CONF,SNC-BD, SNC-LINK, SNC-REF, SNI-BD
pnc-peer	SNI-PEER
procr	PROCR

Category	MO-Type
quick-st	ABRI-PT, ADXDP-PT, ANL-16-LINE, ANL-LINE, ANL-NE-LINE, ANN-PT, ANNOUNCE, ASAI-ADJ, AUDIX-PT, AUX-TRK, BRI-PT, BRI-SET, CDR-LINK, CLSFY-PT, CO-DSI, CO-TRK, CONFIG, DAT-LINE, DID-DS1, DID-TRK, DIG-LINE, DIOD-TRK, DS1-FAC, DS1C-BD, DTMR-PT, EPN-SANITY, EXP-INTF, EXP-PN, FIBER-LINK, GPTD-PT, HYB-LINE, ISDN-LNK, ISDN-TRK, JNL-PRNT, MAINT, MET-LINE, MODEM-PT, OPS-LINE, PDATA-PT, PDMODULE, PKT-BUS, PKT-INT, PMS-LINK, PMS-PRNT, PNC-DUP, PRI-CDR, S-SYN-PT, SN-CONF, SNC-BD, SNC-LNK, SNC-REF, SNI-BD, SNI-PEER, SYS-PRNT, SYSLINK, SYSTEM, TDM-BUS, TDM-CLK, TDMODULE, TIE-DS1, TIE-TRK, TONE-BD, TTR-LEV
sch-adj	SCH-ADJ
s-syn	S-SYN-BD, S-SYN-PT
stabd	ABRI-PORT, ADXDP-BD, ADXDP-PT, ANL-16-LINE, ANL-BD, ANL-LINE, ANL-NE-LINE, ASAI-ADJ, AUDIX-BD, AUDIX-PT, BRI-BD, BRI-PORT, BRI-SET, DIG-BD, DIG-LINE, HYB-BD, HYB-LINE, MET-BD, MET-LINE
stacrk	ADXDP-PT, ANL-LINE, ANL-16-LINE, ANL-NE-LINE, AUDIX-PT, DIG-LINE, HYB-LINE, MET-LINE, OPS-LINE
stations	ABRI-PORT, ADXDP-PT, ANL-16-LINE, ANL-LINE, ANL-NE-LINE, ASAI-ADJ, AUDIX-PT, BRI-PORT, BRI-SET, DIG-LINE, HYB-LINE, MET-LINE, OPS-LINE
sys-link	SYS-LINK
sys-prnt	SYS-PRNT
tdm	TDM-BUS
tone	CLSFY-BD, CLSFY-PT, DETR-BD, DTMR-PT, GPTD-PT, START-E, SYNC, TDM-CLK, TONE-BD, TONE-PT, TTR-LEV
trkbd	AUX-BD, AUX-TRK, CO-BD, CO-DS1, CO-TRK, DID-BD, DID-DS1, DID-TRK, DIOD-BD, DIOD-TRK, DS1-BD, ISDN-TRK, PE-BCHL, TIE-BD, TIE-DS1, TIE-TRK, UDS1-BD, WAE-PT
trkcrk	AUX-TRK, CO-DS1, C9-TRK, DID-DS1, DID-TRK, DIOD-TRK, ISDN-LNK, ISDN-TRK, TIE-DS1, TIE-TRK
trunks	CO-TRK, SUX-TRK, CO-DS1, DID-DS1, DID-TRK, DIOD-TRK, ISDN-LNK, ISDN-TRK, PE-BCHL, TIE-DS1, TIE-TRK, WAE-PORT
vc	VC-BD, VC-DSPPT, VC-LEV, VC-SUMPT
vsp	MMI-BD, MMI-PT, MMI-LEV, MMI-SYNC, VC-LEV, VC-BD, VC-SUMPT, VC-DSPPT, VP-BD, VP-PT, VPP-BD, VPP-PT, DI-BD, DI-PT, MEDPRO, IPMEDPRO, MEDPROPT
wide-band	PE-BCHL, WAE-PORT

Category	MO-Type
wireless	RC-BD, RFP-SYNC, WFB, CAU, WT-STA

5. MO Location: Select an MO Location from the following list:
   - Media Gateway
   - Cabinet
   - Board
   - Port
   - Extension
   - Trunk Group/Member
6. To add the filter, click **Add**.
   The Filters screen appears displaying the new filter.

Changing an SNMP filter

Procedure

1. From the server's Server Administration Interface, click **SNMP Filters** under the Alarms heading.
2. Click the box associated with the filter you wish to change and press **Change**.
3. Make the desired changes to the filter and press **Change**.
   The **Filters** screen appears displaying the changes made to the filter.

Deleting one or all SNMP filters

Procedure

1. To delete all the filters, click **Delete All**.
   The system displays a warning message asking if you are sure. If you wish to continue, click **OK**. The Filters screen appears.
2. To delete one filter, click the box associated with the filter you wish to delete and press **Delete**.

The system displays a warning message asking if you are sure. If you wish to continue, click **OK**. The Filters screen appears with the updated list of filters.

Administering an SNMP Agent

Procedure

1. On the server's Server Administration Interface, click **SNMP Agents**.
2. Check the status of the Master Agent.
   - If the status of the Master Agent is "up": Select Agent Status from the navigation bar and click **Stop Agent**. Once the Master Agent reaches a "Down" state, return to the SNMP Traps screen by clicking **SNMP Traps** on the navigation bar
   - If the Master Agent is in a "Down" state, continue with step 3.
3. In the **IP Addresses for SNMP Access** section:

   Select the radio button associated with one of the following options:
   - No access: This option restricts all IP address from talking to the agent.
   - Any IP access: This option allows all IP addresses to access the agent.
   - Following IP addresses: You can specify up to five individual IP addresses that has permission to access the agent.
4. In the SNMP users/communities section: Select one or more versions of SNMP by clicking on the **Enable** box associated with the version.
   - **SNMP Version 1**:
     i. **Enable SNMP Version 1**: Check this box to enable SNMP v1. If the SNMP v1 box is enabled, SNMP v1 can communicate with the SNMP agents on the server.
     ii. **Community Name (read-only)**: When this option is selected the community or the user can query for information only (SNMPGETs).
     iii. **Community Name (read-write)**: When this option is selected the community or the user can not only query for information but can also send commands to the agents (SNMPSETs).
   - **SNMP Version 2**: Check this box to enable SNMP v2. If the SNMP v2 box is enabled, SNMP v2 can communicate with the SNMP agents on the server.
     i. **Enable SNMP Version 2**: Check this box to enable SNMP v2.

ii. **Community Name (read-only)**: When this option is selected the community or the user can query for information only (SNMPGETs).

iii. **Community Name (read-write)**: When this option is selected the community or the user can not only query for information but can also send commands to the agents (SNMPSETs).

- **SNMP Version 3**: SNMP v3 provides the same data retrieval facilities as the previous versions with additional security. A User Name, authentication password, 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.

  i. **Enable SNMP Version 3**: Check this box to enable SNMP v3. If the SNMP v3 box is enabled, SNMP v3 can communicate with the SNMP agents on the server.

  User (read-only) : Entering a user name, authentication password, and security password in this section provides the user with read functionality only.

  ii. **User Name**: Enter a User Name. The User Name can be a maximum of any 50 characters with the exception of quotation marks.

  iii. **Authentication Password**: Enter a password for authenticating the user. The authentication password must be a maximum of any 50 characters with the exception of quotation marks.

  iv. **Privacy Password**: Enter a password for privacy. The privacy password can contain any 8 to 50 characters with the exception of quotation marks.

  User (read-write): Entering a user name, authentication password, and security password in this section provides the user with read and write functionality.

  v. **User Name**: Enter a User Name. The User Name can be a maximum of any 50 characters with the exception of quotation marks.

  vi. **Authentication Password**: Enter a password for authenticating the user. The authentication password must be a maximum of any 50 characters with the exception of quotation marks.

  vii. **Privacy Password**: Enter a password for privacy. The privacy password can contain any 8 to 50 characters with the exception of quotation marks.

5. To save the changes, click **Submit**.
6. Once you are finished adding the SNMP Agent, you must start the Master Agent.

To start the Master Agent, select **Agent Status** from the server's Server Administration Interface and click **Start Agent**.

Important:

You can use the Agent Status screen to change the state of the Master Agent and to check the state of the subagents. If the subagent is connected to the Master Agent, the status of each subagent is "Up." If the status of the Master Agent is "Down" and the status of the subagent is "Up," the subagent is not connected to the Master Agent.

Viewing and modifying agent status

The Agent Status Web page shows the current state of the Master Agent and all of the sub agents. Use this page to to start or stop the Master Agent.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Server (Maintenance)** > **Agent Status**.
   The current status of the Master Agent and Sub Agents is displayed on the Agent Status page. If the status of the Master Agent is **Up**, the page displays **Stop Agent** button. If the status of the Master Agent is **Down**, the page displays the **Start Agent** button.
2. To modify the status, click **Stop Agent** or **Start Agent**.

Chapter 14: Logs

Logs

The system uses a series of logs as the central collection point for information flowing from all of the messaging features and feature packages. These logs provide a systemwide view of activities, errors, and alarms.

Messages in the logs range in importance from informational to critical. The logs vary based on audience (login type) and information type. The current system uses four logs:

User Activity Log The 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 subscriber-reported problems. The activity log is accessible to the vm, sa, and craft logins.

Administrator's log The administrator's log records informational messages that could require some action by the messaging system administrator. These messages might simply log a successful nightly backup, or they could 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 The alarms signal a service-affecting or potentially service-affecting problem with the system. The alarm log records major, minor, and warning alarms generated by the system. The system automatically notifies a designated remote service center of all major and minor alarms by using the modem if the system is registered with the Avaya Remote Service Center. The customer is responsible for resolving all warning alarms. The alarm log is accessible to the vm, sa, and craft logins.

Maintenance log The 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.

Viewing system logs

The System Logs Web page provides logs for multiple purposes, such as reporting network problems, security issues, system reboots, and so on. 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:
   - **Log types**
   - Select a view from the options provided in **Select a View**.
3. Select an event range.
4. (Optional) To further limit your search, select **Match Pattern** check box and enter a keyword in the field (such as a name or message type).
5. Select display options from **Display Format:**
   - Enter the **Number of Lines** you want to view at one time.
   - To view the most recent text line, select **Newest First**.
   - Likewise, to view without the header, click **Remove Header**.
6. Click **View Log**.

System logs field descriptions

Field	Description
lm	Log Manager Debug Trace (default). Provides information about Messaging and High Availability Platform software, such as restarts, initializations, and shutdowns, process errors, system alarms, and communication with external gateways and port networks. The log rolls over when it reaches its size limit.
lxsys	Linux syslog. This log is used by Linux and platform software. It includes Messaging boot information, kernel messages, platform alarms, Messaging alarms, Messaging IP events (if enabled), cron jobs, and general Linux information messages.

lxsec	Linux Access Security log. This log contains Information pertaining to log-on connections to the Linux system. Actions logged in this file include opening or closing an SSH session and modem messages.
lxwtmp	Linux login/logout/reboot log. This log contains information about Linux log-on and log-out procedures, as well as system reboots.
lxxfer	Linux File Transfer log. This log contains information about files copied to or retrieved from the system. It indicates, among other things, the time, user, and files that were copied to or retrieved from the system.
wd	Watchdog logs. Only the watchdog process writes to this log. It contains information about application starts, restarts, failures, shutdowns, heartbeating, and Linux reboots. It also contains information about processes that use excessive CPU cycles. The watchdog logs do not contain much specific information about Messaging. If you need information about processes relating to call processing, view the logmanager debug trace log.
cmds	Platform Command History log. This log contains information about Web page access, Web page activity, and bash commands. Use the “bashhist” view to display just the bash commands.
httperr	HTTP/Web server error log. These are errors and events generated by the platform Web server and include items like Web server restart, abnormal CGI script file terminations, and certificate mismatches.
httpssl	HTTP/Web secure sockets layer (SSL) request log. These are all the requests made of the Web servers SSL module. All pages requested or placed in secure mode are indicated.
httpaccess	HTTP/Web access log.
cmrestart	This log contains the last 16 restarts of the server restart. including the level, why they were requested, and whether they were escalated.
filesync	Messaging file synchronizations log.

View	Description
ipevt	IP events, such as interfaces up/down and telephone or endpoint registration or unregistration. These are events that the server posts through Messaging. For **IF_UP/IF_DOWN** the following fields are displayed: 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

View	Description
bashhist	Platform bash command history log. This log lists the commands run by interactive bash cells. These commands include: **PPID**:The process ID of the parent shell. **PID**: The process ID of the shell. **UID**: The user ID under which the shell is executing. Zero (0) means root or super user.
kernel	Linux kernel debug messages. These messages contain debug information about the driver, disk, hardware, and memory.
cron	Linux scheduled task log (CRON). This log shows information from the Linux scheduling daemon.
mst	Messaging 's Message Sequence Trace (MST) log. If enabled through a SAT command, entries to the message sequence trace (MST) log can be repeated into the debug trace log in a format somewhat readable.
mt	Messaging processed Message Tracer (MDF).
mta	Messaging interpreted Message Tracer (MTA).
hwerr	Messaging hardware error and alarm events. These events go into the Messaging harware error and alarm logs.
sat	Messaging SAT events. These events are created by Messaging for SAT activity. The entries contain the name of the process that creates the entry, the login name, an action, such as change, display, test, and list, an object, such as station, trunk, and a field name.
swerr	Messaging software events. The events that go into the Messaging software error log. This needs special deciphering by an external tool.
update	System update/patch events. The update tool events include the following information: • Type of the update tool script used for a particular update file • Additional information about certain update tool scripts (activate/deactivate) indicating if a process stopped and restarted • Status of the update tool indicating if the update tool ran successfully
denial	Messaging denial events. Shows the denial events on the system. These events are not software errors, but unexpected events caused by mismatched translation, mismatched provisioning, network problems, invalid operation, resource exhaustion, and so on.

System log results

When you click **View Log** from the System Logs page, the results you see vary depending on which of the following logs you chose.

Logmanager debug trace log

Results for the logmanager debug trace log use the following format:

```
yyyymmdd:hhmmss[milliseconds]:sequence number:process name (process
ID):priority:message
```

For example:

```
20020628:162547538:100:LIC(13648):HIGH:[...license server
initializing...]
```

where:

20020628 is the date.

162547538 is the time (16 hours, 25 minutes, 47 seconds, 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.

Operating system boot messages log

Results for the operating system boot messages log use the following format:

```
yyyymmdd:hhmmss.milliseconds:sequence number:message type:priority:[machine
name] [process name]:message
```

For example:

```
20021028:184554.000:1:lxboot:MED:chenpc rc:Stopping keytable
succeeded
```

where:

20021028 is the date.

184554.000 is the time (18 hours, 45 minutes, 54 seconds, 000 milliseconds).

1 is the sequence number.

lxboot is the message type.

MED is the priority.

chenpc rc is the machine name, followed by the process name (rc).

Stopping keytable succeeded is the message.

Linux scheduled task log (CRON)

Results for the Linux scheduled task log use the following format:

```
yyyymmdd:hhmmss.milliseconds:sequence number:message type:priority:message
```

For example:

```
20021028:040500.000:1:lxcron:MED:root 1209) CMD (/opt/ecs/sbin/
filesync -st all)
```

where:

20021028 is the date.

040500.000 is the time (04 hours, 05 minutes, 00 seconds, 000 milliseconds).

1 is the sequence number.

lxcron is the message type.

MED is the priority.

root 1209 is the login that executed the scheduled task and the process ID.

`CMD (/opt/ecs/sbin/filesync -st all)` is the command that the scheduled task executed.

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.
```

where:

20021104 is the date.

112113.000 is the time (11 hours, 21 minutes, 13 seconds, 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)
```

where:

20020102 is the date.

115000.000 is the time (11 hours, 50 minutes, 00 seconds, 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 log came.

PAM_*pwdb[29937]* is the application that logged the message, followed by its process ID (pwdb[29937]).

(rsh) session opened for user xyz_login by (uid=25) is the description of what the process did or executed.

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)
```

where:

20021101 is the date.

170800.000 is the time (17 hours, 08 minutes, 00 seconds, 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 an IP address may be indicated.

`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 will show “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
```

where:

20020114 is the date the ftp transfer took place.

1 is the sequence number.

090716.000 is the time the FTP transfer took place (09 hours, 07 minutes, 16 seconds, 000 milliseconds).

:: means the field is unused.

MED is the priority.

rem.servername.com is the remote host name. Instead of the host name an IP address may be indicated.

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. The “b” refers to a binary transfer; an “a” refers to an ASCII transfer.

_ is the special action taken. In this case, the“” indicates that no action was taken.

o is the direction of the transfer. The “o” means that the transfer was outgoing; an “I” means that the transfer was incoming.

a is the method by which the user logged in. In this case, the “a” means the user logged in using an anonymous login.

smith@mycompany.com is the local user name. If the user is logged in using an anonymous or guest login, this field contains the ID string given when the password was entered (typically an e-mail address).

ftp (file transfer protocol) is the name of the service being invoked.

Note:

Data is recorded in a log file when invoking an FTP session from a remote PC to the host server using an anonymous login. Conversely, data is not recorded in a log file when invoking an FTP session from the host server to a remote PC.

0 is the method of authentication used. The “0” means that no authentication method was used.

* is the user ID returned by the authentication method. The “*” indicates that an authenticated user ID is not available.

c is the status of the transfer. The “c” means the transfer was completed; 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
```

where:

20020521 is the date when the command was issued.

164138.928 is the time (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
```

where:

20021023 is the date.

020500.000 is the time the server command was issued.

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

The Storage server logs are organized as follows:

- Administrator’s log: Identifies system events. These events include problems that you need to correct. Some events, such as full subscriber mailboxes and undeliverable messages, directly affect message processing.
- Alarm log: Lists active or resolved messaging system alarms. The most severe alarms are always listed first since these are most often the cause of the problem.
- Maintenance log: Contains descriptions of all reported maintenance events.
- 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 that were run, or changes to software.
- Enhanced-List Application (ELA) Delivery Failure log: Provides information on failed ELA deliveries.
- Software Management log: Contains information about the installation, update, and removal of software packages.
- IMAP or SMTP Messaging log: Contains information about the status of each e-mail process.
- User Activity: You can use this log to track a specific subscriber activity by extension and time, and you can often resolve reported problems by observing the Activity Log before filing a trouble report.

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 it 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, access 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 appropriate information in the fields.
   For more information, see Administrators log field descriptions on page 181.
3. Click **Display**.

Administrators log field descriptions

Field Name	Description
Start Date:	The beginning date for the log report. If you leave this field blank, all qualifying logs are displayed. The default value is the date that this page was last used.
Time:	The beginning hour and minute that the report begins. The **Start Date:** field must have valid entries before you can use this field. If the **Time:** field is blank, all alarms for the specified start date are displayed.
Application:	The two-character application code for the administration log entry: (blank): All applications AS: Access Security Gateway EL: Enhanced List Application MT: Maintenance SM: Station Manager SW: Switch Integration VM: Messaging VP: Voice Platform
Event ID:	The event ID for a specific event. A blank field displays all event types.
Search String:	A text string that you want the system to search for in the administrators log entries. The system searches the **Message** field of the administrators log for matching text.

Checking the alarm log

About this task

The alarm log contains descriptions of all significant problems detected by the system including active alarms and resolved alarms. These are alarms that are corrected either automatically or by repair procedures.

Note:

You must check the alarm log on a daily basis.

Procedure

1. On the Administration menu, click **Messaging** > **Logs** > **Alarm**.
2. Enter appropriate information in the fields.
   For more information, see Alarm log field descriptions on page 182.
3. Click **Display**.

Alarm log field descriptions

Field Name	Description
Alarm Type	Alarm type to display. The options are: • Active • Resolved
Alarm Level Major?:	Indicates if Major alarms are to be displayed. The options are: • Yes • No
Alarm Level Minor?:	Indicates if warning alarms are to be displayed. The options are: • Yes • No
Alarm Level Warning?	Indicates if you want to display warning alarms. Select Yes or No.
Start Date	Indicates the start date for the logs to be generated. Start Date is in MMDDYY format. For active alarms, the date

Field Name	Description
	specifies when the alarms were raised. For resolved alarms, the date specifies when the alarms were resolved.
Time	Indicates the starting time for generating the logs. 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 date specifies when the alarms were resolved.
Application	A two-character application ID that identifies each module in the system. Log entries with only the specified Application ID are displayed. The IDs are: • EL: Enhanced List Application • LD: LDAP • MT: Maintenance • SM: Station Manager • SW: Switch Integration • VM: Messaging (voice mail, fax mail, and email messages) • VP: Voice Platform
Resource Type	Alarmed resource type. This identifies the generic alarmed resource type that requires maintenance action. Log entries with only for the specified alarmed resource type are displayed.
Alarm code	Alarm code identifies the reason for the alarm against the specific resource.

Viewing maintenance logs

You can view the descriptions of all reported maintenance events on the maintenance log page.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Logs** > **Maintenance**.
2. Enter appropriate information in the fields.

For more information, see Maintenance log field descriptions on page 184

3. Click **Display**.

Maintenance log field descriptions

Field Name	Description
Errors?	Indicates if the log entries with the event type ERR will be displayed.
Resolutions?:	Indicates if the log entries with the event type RES will be displayed.
Events?:	Indicates if the log entries with the event type EVN will be displayed.
Start Date:	Indicates the start date for generating the logs. The logs for the specified date and forward gets displayed. The year field requires two characters. The numbers 00-37 represent the years 2000 - 2037, and numbers 70-99 represent the years 1970-1999.
Time:	Indicates the start time for generating the logs. The logs are generated for the specified time and forward. If you do not specify the time, the time of the day indicated as 00:00:00 is considered 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: • (blank): All applications • AS: Access Security Gateway • MT: Maintenance • SM: Station Manager • SW: Switch Integration • VM: Messaging • VP: Voice Platform
Event ID:	Identifies the reported event. Log entries with the specified Event ID code are displayed.
Problem Resource Type:	This identifies the logical resource type or system component reported. Only log entries with the specified problem resource type get displayed.

Field Name	Description
Reporting Resource Type:	Identifies the logical resource type of the resource that discovers and detects the problem. Only log entries with the specified reporting resource type are displayed.
Reporting Resource Source:	Identifies the specific line of code reporting the condition. Only log entries with the unique value used to display the specified reporting resource source are displayed.
Search String:	Enter a text string. Only log entries that contain the specified text entries are displayed.

Viewing administration history log

About this task

The Administrator's History log identifies administrative events that occur on your system. These events include information about any changes to your system, such as logins, command line entries, reports that were run, or changes to software.

Procedure

1. On the Administration menu, click **Messaging** > **Logs** > **Administration History**.
   The system displays the Administration History Log page.
2. Complete the fields on this page.
3. Click **Display** to generate the report.

Administration history log field descriptions

Field Name	Description
Start Date:	The beginning date for the log report. If you leave this field blank, all qualifying logs are displayed. The default value is the date that this page was last used.
Time:	The beginning hour and minute that the report begins. The **Start Date:** field must have valid entries before you can use this field. If the **Time:** field is blank, all alarms for the specified start date are displayed.
Application:	The two-character application code for the administration log entry: (blank): All applications

Field Name	Description
	AS: Access Security Gateway EL: Enhanced List Application MT: Maintenance SM: Station Manager SW: Switch Integration VM: Voice Messaging VP: Voice Platform
Event ID:	The event ID for a specific event. A blank field displays all event types.
Search String:	A text string that you want the system to search for in the administrators log entries. The system searches the **Message** field of the administrators log for matching text.

Viewing ELA delivery failure logs

About this task

The Enhanced-List Delivery Failure Log page provides information on failed ELA deliveries.

Procedure

On the Administration menu, click **Messaging** > **Logs** > **ELA Delivery Failures**.

ELA delivery failure log field descriptions

Field Name	Description
Date:	Date of failure delivery.
Time:	Time of failure delivery.
Message Originator	Mailbox number of the originator of the failed message.
Parent List	The Enhanced-List to which the originator sent the message. The Parent List may be a local or remote list mailbox.
Child List	The last Enhanced-List visited in a nested Enhanced-List hierarchy before the message failed. The Child List is always a local mailbox. If the Enhanced-Lists are not nested, the Child List is the same as the Parent List.
Failed Recipient	Name of the intended recipient of the failed message.

Field Name	Description
Failed Address	Mailbox number of the intended recipient of failed message. Note that the Failed Address may be the system broadcast mailbox.
Failure Reason	Detailed reason for the delivery failure.

Viewing software management logs

About this task

The Software Management Logs page displays information on software installation, update, and removal.

Procedure

1. On the Administration menu, click **Messaging** > **Logs** > **Software Management**.
2. Select a log to view from the **Select a log to view** drop-down list.

   For more information, see Software management log field descriptions on page 187.

Software management log field descriptions

Field Name	Description
Installation/Removal Log.	A log of the most recent software installation, update, or removal session.
Old Installation/Removal Log	A cumulative log of old software installation, update, and removal sessions. Old sessions appear in this log, beginning with the most recent old session. When a new session begins, the most recent installation, update, or removal session log is moved to the beginning of this log.
Summary of Installation/ Removal of Packages.	A cumulative, detailed log of software package component installation and removal attempts. The success or failure of each attempt is recorded for each set and set member.

Viewing Internet messaging logs

About this task

The Internet messaging logs contain information about occurrences at each stage in the messaging process.

Procedure

1. On the Administration menu, click **Messaging** > **Logs** > **IMAP/SMTP Messaging**.
2. Select a type of log to view from the **Select log to view** drop-down list.
3. To clear the logs from the page, click **Clear the Log**.

   For information on the fields, see Internet messaging log field descriptions on page 188.

Internet messaging log field descriptions

Field Name	Description
User Agent Log	Software interfaces called delivery agents are required for the message transport agent (MTA) to function with the user agent (UA).
Remote Delivery Agent Log	Accepts messages from the User Agent through the Outbound queue and delivers them to the Queuer.
Local Delivery Agent Log	Accepts messages from the MTA through the Dispatcher. Passes incoming messages to the UA through the Inbound queue.
Queuer Log	Accepts messages from the RDA and either passes them to SMTP Out or stores them in the SMTP queue until they can be accepted.
Dispatcher Log	Accepts messages from SMTP In and passes them to the LDA, or stores them in the SMTP queue until they can be accepted.
SMTP In Log	Transfers incoming messages from the Internet to the Dispatcher.
SMTP Out Log	Transfers outgoing messages from the Queuer to the Internet.

Field Name	Description
Administration/Event Log	Records occurrences that are informational or that requires administrator intervention.
IMPAP4 Log	Records errors and events occurred in the communication between users POP3 and IMAP4 clients 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 errors and events that may occur in the communication between users' POP3 and IMAP4 clients and the message server. Additional information includes errors and significant events dealing with the server and the rest of the messaging system.

User activity logs

The user activity log is an administrative tool useful for investigating reported problems with message delivery and the operation of the message-waiting indicator (MWI). The activity log maintains a history of the activity on the Messaging system. You can use this log to track a specific users activity by extension and time, and you can often resolve reported problems by observing the activity log before filing a trouble report.

Configuring user activity log

Procedure

1. On the Administration menu, click **Messaging** > **Messaging System (Storage)** > **User Activity Log Configuration**.
2. Enter appropriate information in the fields.

   For more information, see Configure user activity log field descriptions on page 190.
3. Click **Save**.

Configure user activity log 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 whether the entries in the activity log will be reset.

Running an activity log report

Procedure

1. On the Administration menu, click **Messaging** > **Logs** > **User Activity**.

   Note:

   This report can take several minutes to run depending on the system load and the size of the log file.

2. Select the duration from the **Start Date** and **End Date** fields for which you want to view the users activity.
3. Click **Display**.

User activity log field descriptions

Field Name	Description
Mailbox Number	Mailbox number of a user on the system.
Start Date	Start date for generating logs. Log entries for the specified date and forward get displayed.
End Date	End date for generating logs. Log entries up to the specified date get displayed.
Time:	Time in hours and minutes for generating the logs.
Date	Date when the activity was logged.

Field Name	Description
Time	Time when the activity was logged.
Activity	Type of activity logged into the system.
Description	Description of the logged activity.

Application server logs

Application Server logs overview

The Application Server provides the following logs:

- System Log Filter: Provides access to the full system log, with advanced filtering options to zoom in on specific constraints. All displayed times reflect the time zone of the Application Server.
- Call Records: Shows all incoming and outgoing phone activities on the Application Server. All displayed times reflect the time zone of the Application Server. Current phone logs are rotated on a monthly basis. The Current Log section shows the phone log for the current month.
- Reporting Logs: There are two types of logs:
  - Audit Log: The audit log is a historical log of Application Server cluster configurations. It tracks all configuration changes made to the system over time. All displayed times reflect the time zone of the Application Server. The details of the audit log include date and time of change, the changed object, and the new value to be assigned.
  - Port Usage Logs: Port Usage logs are created and saved daily on the Application Server in comma-separated value (.csv) format. All displayed times reflect the time zone of the 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. Diagnostics log files are deleted from the Application Server after 14 days.
- Call Logs: The call logs provide traces of individual calls for application tuning.

Configuring log settings

Procedure

1. On the Administration menu, click **Messaging** > **Server Settings (Application)** > **Log Configuration**.
2. Select a **System Logging Mode**.

   By default, this mode is set to **Normal**. When testing the configuration, you can temporarily select **Testing** for more detailed logging.

   For detailed troubleshooting, select **Debug** or **Extensive**. These logging modes must be selected when advised to do so by qualified support personnel. These logging modes may generate logging data that could impact system performance.
3. Click **Apply**.

Running system log filter

The System Log Filter page provides access to the full system log, with advanced filtering options to zoom in on specific constraints.

Procedure

1. On the Administration menu, click **Messaging** > **Logs** > **System Log Filter**.
2. Enter appropriate information in the fields.

   For more information, see System Log Filter on page 193.
3. Click **View**.

System Log Filter

Field	Description
Date interval	With the default settings, the log filter shows all events for the last day. The options are: • To change the date interval for the log filter, select a different value in the **Date Interval** drop-down list. • Select **Specific** to define a specific interval (in the **Start Date** and **End Date** fields) or select one of the predefined intervals. • To not filter based on date, select **All**.
Category	System component to filter the system log by. The options are: • All • Voice Browser • Infobridge • Health Monitor • Cache • Configuration • Hardware • Telephony Integration Summary • Telephony Integration Details • Exchange Integration
Severity	Severity level to filter the system log by. The options are: • All • Err • Warning • Notice • Info • Debug
Phone Line (optional)	Affected phone line to filter the system log.
Session ID (optional)	Session ID to filter the system log by.

Field	Description
Tag (optional)	This field is currently unused.
Number of lines in log to filter (optional):	Number of lines in the log where the filter can be applied.

Note:

Filtering based on Phone Line, Session ID, and Tag are only relevant for certain log events and are typically only used by qualified support personnel.

Collecting system log files

Use this page to download application server system log files. You can download the log files for the last hour or for a specific time duration.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Logs** > **Collecting system log files**.
2. For **Date Interval**, select any one of the following:
   - **Last Hour**
   - **Specific** and provide **Start date**, **End Date**, and **Time**
3. Click **Download**.
   System prompts you to download the zipped log file.
4. Save the system log file.

Viewing call records

Use this page to view the call records showing all incoming and outgoing calls on the application server. All displayed times reflect the time zone of the server. Current call records are rotated on a monthly basis. The **Current Log** section shows the call records for the current month.

The phone logs call record format is displayed in XML, with LOG_ENTRY entries for each call record.

Note:

For an incoming call that also generates an outgoing call, the outgoing call record is logged before the incoming call record.

About this task

Procedure

On the Administration menu, click **Messaging** > **Logs** > **Call Records**.
The **Current log** appears.

Viewing audit and ports usage

The audit log is a historical log of cluster configurations. It tracks all configuration changes made to the system over time. All displayed times reflect the time zone of the application server. The details of the audit log include date and time of change, changed object, and the new value to be assigned. Port Usage logs are created and saved daily on the application server in comma-separated value (.csv) format. The best way to use these logs is to save a log file locally, and then display it.

Procedure

1. On the Administration menu, click **Messaging** > **Logs** > **Audit/Ports Usage**.
2. Select one of the following as required:
   - To view the audit log, click **configd-audit.log**.
   - To view a port usage log, click the port usage log (.csv) you want to view.
3. Select a location in the Save As dialog box and click **Save**.
   The log is best viewed using a structured text editor (for example, TextPad).

Note:

For assistance, contact Avaya Client Services.

Accessing diagnostics results

The Diagnostics Logs page provides access to the results generated by the Application Server diagnostics. Time stamps of the logged files reflect the time zone of the Application Server. All diagnostics results for a given day are stored in a single log file. Diagnostics log files are deleted from the Application Server after 14 days.

Procedure

On the Administration menu, click **Messaging** > **Logs** > **Diagnostics Results (Application)**.

The Diagnostic Logs page appears with a list of diagnostic logs generated through the **Messaging** > **Diagnostics** > **Diagnostics (Application)** page.

For information on running the diagnostics, see Running application server diagnostics on page 214.

- To download all the diagnostic logs as on zip file, click **Download**
- To download a specific diagnostic log, click the particular log.

Chapter 15: Reports

Reports overview

You can use the System Management Interface 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 attributes. It also collects information that depicts how the system is used, including data about features, users, communities, data port loads, and remote-messaging traffic. Messaging displays this information in real-time dynamic report pages and in messaging traffic reports.

Report	Description
User report	Provides a summary of Users (Local), Locked Out Users, Uninitialized Users, Remote Users, and Login Failures.
System Evaluation report	Provides a summary of various Messaging settings and attributes. This report also shows information about dormant mailboxes. A dormant mailbox is a mailbox that has not been accessed in 30 days, or a new mailbox that has not received any messages in 30 days.
Internet Messaging Traffic	Provides a summary of the port usage on the Messaging system in daily or hourly periods. This reports helps to determines if the Messaging system is performing at peak efficiency by providing actual usage information. This report also provide the information about outcalling ports, user traffic, and feature traffic that helps to evaluate system efficiency.
TCP/IP Snapshot	Provides the total traffic for all the machines with the specified connection type. Also displays the total number of updates.
Measurements	Shows daily measurements of messages that were sent and received by each community.

Viewing user reports

The Reports page displays different types of dynamic information about users, including:

- Users (Local)
- Locked Out Users
- Uninitialized Users
- Remote Users
- Login Failures
- Information Mailboxes

For information about the individual reports, see Reports field descriptions on page 198.

Procedure

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

You can change the display by changing the setting in the **Report** drop-down list.

Reports field descriptions

Name	Description
Users (Local)	A list of local users added to the Messaging system
Locked Out Users	A list of users that have been locked out of the Messaging system. A user on this list can be unlocked by accessing the User Properties page for the user and unchecking the Locked out from voice messaging check box.
Uninitialized Mailboxes	A list of users who have been enabled to use voice messaging, but who have not completed initializing their mailbox. Initialization of a mailbox includes: **Password Initiation**: A new user is provided with a temporary password that needs to be changed at the first logon though the TUI or the User Preferences page. Users will not be able to listen to voice messages without logging on to the system and changing their temporary password. **Name Recorded**: New users are asked to record their names when they log on to the

Name	Description
	TUI for the first time. The recorded name is what callers hear in the Auto Attendant. **Greeting Recorded**: When users log on to the TUI for the first time they are asked to record a personal greeting. This greeting played to the callers when their call is not answered by the user.
Remote Users	A list of remote users in Messaging system.
Login Failures	A list of users with failed login authentication attempts.
Information Mailboxes	A list of info mailboxes in the Messaging system.

Running system evaluation report

This page displays a summary report of various system settings and attributes. Depending on the system, the summary report displays different types of dynamic information.

Procedure

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

   The **System Evaluation Report** runs automatically when you click System Evaluation (Storage).

2. To refresh the report, click **Re-run System Report**.

   The System Evaluation Report page displays the following information:

   - System Status
   - Site Information
   - Software Summary
   - Hardware Summary
   - Reliability Information
   - Networked Machines, if administered
   - Extension Ranges
   - File System Usage

- Installed Software Packages

Running traffic measurement reports

Use the Measurements page to request traffic measurements from the Messaging system.

Procedure

1. On the Administration menu, click **Messaging** > **Server Reports** > **Measurements (Storage)**.
2. On the Messaging Measurements page, select the appropriate information.
3. Click **Get Report**.

   For more information on the fields, see Measurements field descriptions on page 200.

Measurements field descriptions

Name	Description
Type	The types of traffic include: **Community**: The traffic by community. **Feature:** : The traffic information for messaging features . **Load**: The traffic for user thresholds and voice ports. **Network-Load**: The traffic for network measurements and port usage. **Remote-Messages**: The message and session traffic for remote machine. **Special-Features**: The outcalling traffic **User**: The user traffic **Traffic-Snapshot** : A snapshot for all remote machines.

Name	Description
Cycle	Indicates the frequency type to sample. The frequency types you can select are determined by the traffic type. The frequencies that might be available for selection are hourly, daily, or monthly.
Date	Date to start sampling.
Hour	Hour to start sampling.

Viewing TCP/IP Snapshot

This page displays status of Outgoing Connections and Incoming Connections.

About this task

To view the TCP/IP Snapshot:

Procedure

On the Administration menu, click **Messaging** > **Reports** > **TCP/IP Snapshot**.

The TCP/IP Snapshot page displays the following information for **Outgoing Connections** and **Incoming Connections**:

- Machine
- Last Connection
- Status
- Retry

Chapter 16: Maintenance

Performing voice messaging database audit

During normal operation, 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 databases are handled separately, it is possible for one database to contain information that conflicts with another database. For example, if a user is removed from the Messaging database, other databases could still contain messages addressed to that user or mailing lists that include that deleted user's name. Audits can reconcile such conflicts among databases to check for inconsistencies and when possible update information in databases to correct Messaging problems. For example, audits remove all references to a deleted user, which includes deleting the user's name from mailing lists and canceling message deliveries to that user. Audits run automatically or can be performed on demand as well.

About this task

All of the voice messaging database audit types use the same general procedure.

Procedure

1. On the Administration menu, click **Messaging** > **Utilities** > **Messaging DB Audits (Storage)**.
2. Click one of the links from the following table for that audit:

   Voice Messaging Database Audits

To Audit	Click
View Audit History	**History**
Mailboxes	**Start Mailboxes Audit (Mailboxes, Mailbox Data)**
Mailing lists	**Start Mailing Lists Audit (Mail Lists, Delivery Data)**
Names	**Start Voice Names Audit (Voice Names)**
Network data	**Start Network Data Audit (Machine Translations, Network Translations, Network Data)**

To Audit	Click
	Note: This audit is available only if the system has Digital Networking.
Subscriber data	**Start Subscriber Data Audit (Subscribers, Delivery Data)**
Nightly Audit	**Start Subscriber Data Audit (Subscribers, Delivery Data)**
Weekly Audit	**Start Weekly Audit (Weekly, Delivery Data, Network Data, Mailbox Data)**

The system displays the audit name and Result code, which indicate that the audit is running.

3. Wait for the audit to finish or take one of the following steps:
   - Click **Abort** to partially stop the audit and exit the page.
   - Click **Back** to go to the Audits 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.
   c. If the system is not providing service and the remote service center cannot help immediately.

IMAP/SMTP administration

Administering General Options and Settings

Use the fields on this page to manage the amount of messaging resources devoted to e-mail processing. The fields also define how Internet Messaging affects other messaging features.

Procedure

1. On the Administration menu, click **Messaging** > **IMAP/SMTP Administration** > **General Options**.
2. Select **Maximum number of INCOMING SMTP sessions**.

3. Select **Maximum number of OUTGOING SMTP sessions**.
   For more information, see General Options field descriptions on page 205.
4. Click **Save**.

General Options field descriptions

Name	Description
Maximum Number of INCOMING SMTP Sessions	SMTP sessions require processing resources and affect the quality of service. If several e-mail messages are received simultaneously, additional sessions are started to accommodate the additional traffic, up to the administered limit. Increasing this number limits the possibility of a sending machine being temporarily unable to send e-mails. Although most e-mail servers retry automatically, many e-mail clients require users to resend the message. After setting this field and turning on Internet Messaging, check the volume of e-mail traffic under the SMTP Outgoing option by selecting **Reports** > **SMTP Log Summary**.
Maximum Number of OUTGOING SMTP Sessions	The maximum number of sessions are used only if needed. If a large volume of outbound e-mail is queued for delivery, additional sessions are started, up to the administered limit. After setting this field and turning on Internet Messaging, watch the volume of e-mail traffic under the SMTP Outgoing option by selecting the **Reports** > **SMTP Log Summary**

Configuring Mail Options

Use this page to specify how e-mail is managed and to define configuration information that is used in processing incoming and outgoing e-mails.

Depending on the selections you make on this page, the outgoing e-mail address is resolved as follows:

- If a Mail Gateway is used, all outbound e-mails are sent to the gateway for delivery to the eventual destination
- If a Mail Gateway is not used, the configured Domain Name Server is used to look up the host.domain portion of the outgoing user@host.domain e-mail address.
- If the DNS lookup fails, the administered Host File entries are checked for this host.domain.
- If these methods fail, the message is marked undeliverable and returned to the sender.

Procedure

1. On the Administration menu, click **Messaging** > **IMAP/SMTP Administration** > **Mail Options**.
2. Enter appropriate information in the fields.
   For more information, see Mail Options field descriptions on page 207.
3. Click **Save**.

Adding a mail gateway

About this task

A mail gateway enables Messaging to connect to other mail systems. It also enables the storage server to send text notifications. For more information, see Network overview on page 5.

Procedure

1. On the Administration menu, click **Messaging** > **IMAP/SMTP Settings (Storage)** > **Mail Options**.
2. In the **Maibox Gateway Machine Name** field, select the host name that you entered in Administering the external SMTP host on page 22.
3. Keep the **Server Alias** blank.
4. Click **Save**.
   For more information, see Mail Options field descriptions on page 207.

Next steps

Configure a trusted server. See Configuring a trusted server on page 23.

Mail Options field descriptions

Name	Description
Mail Gateway Machine Name	The TCP/IP host name for mail gateway. Your communication network routes all outbound mail through the gateway you select from this drop-down list. The list is populated from the Administer External Hosts page. Example: 94221@machine.domain.com
Server alias	An alternate host name for the mail gateway. Example: 94221@domain.com Aliases allow organizations to create easily recognized e-mail. addresses for their clients and employees. Example: extension@domain
Warn about undeliverable mail after	The number of days after which users are notified that their message has not been delivered. Internet Messaging attempts delivery for the specified number of days. Then, the sender receives a warning that includes a part of the message for identification purposes. Attempts to deliver the message continue even after the warning notification. The number of times the server attempts delivery depends on the number of days set in this option.
Report undeliverable mail and delete it after	The number of days after which an undeliverable message is returned to the sender. After this threshold is passed, the sender receives an e-mail that the message was undeliverable. The original message is attached. Message delivery is no longer attempted.
Check for new mail every	The time interval for checking the message queues. Outgoing and incoming messages are sent and delivered immediately. However, if a message is not sent or delivered immediately, the system will perform a check after the specified interval and deliver all messages in the queue.

Verifying IMAP/SMTP status

This page displays the latest snapshot about the Internet Messaging operation.

The **IMAP/SMTP Status** page displays the following information:

- **Internet Message status:** Displays whether the inbound and outbound mail delivery processes are operating.
- **Percent of media space in use (contains queues):** Displays the percentage of used space in the media file system. The media file system contains messages and various system data, including temporary files, Internet Messaging queues, and logs.
- **Number of incoming messages in queue:** Displays the actual number of messages waiting in the incoming message queue when the data was read. This value is affected by the setting of the incoming SMTP sessions field on the SMTP Options page. If the setting is high, more messages are allowed into the queue and use more space. If too much space is used, message storage or processing gets affected.
- **Number of outgoing messages in queue:** Displays the actual number of messages waiting in the outgoing message queue when the data was read.
- **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 e-mail 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.

Procedure

On the Administration menu, click **Messaging** > **IMAP/SMTP Administration** > **IMAP/SMTP Status**.

Voice equipment diagnostics

Voice Equipment Diagnostics

You can perform the following diagnostics on an installed analog-line interface card:

- Busying out voice channels on page 209.
- Diagnosing the voice equipment on page 210.
- Displaying voice equipment status.
- Releasing voice channels on page 213.

Busying out voice channels

Busying out voice channels takes all channels out of service. Calls do not get forwarded out of service channels. You can busy out more than one channel.

Note:

Do not busy out all voice channels at once or there will be no channels left for incoming calls.

Procedure

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

   For more information, see Busy out voice equipment field descriptions on page 210.
3. Click **Busyout**.
4. When the state change is complete, the system displays the Busyout of Voice Equipment results page.

Busy out voice equipment field descriptions

Field Name	Description
New State	Specifies the state of the equipment. This field is always **manoos**.
Equipment	This field is always **Channel**.
Equipment Number	Specifies the number of the channel. Enter a valid number or range or all. You can enter channel numbers in several forms: A single number (for example, 1) A range of numbers (for example, 0-2) A list of single numbers (for example, 0,1,2) A list of single numbers and ranges (for example, 0, 1-2)
Change Immediately?	Select **YES** to change the state immediately, even if the channel is busy, or **NO** to change the state when the channel becomes idle. Caution: Selecting **YES** in the Change Immediately? field disconnects 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 they are free of calls. Busying out voice cards and channels only when they are free of calls can take longer, but calls are not disconnected.

Diagnosing voice equipment

About this task

To diagnose voice channels or cards:

Procedure

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

   Diagnose voice equipment field descriptions on page 212.

Note:

Do not diagnose all the analog-line interface cards or channels at once or there will be no available channels to accept incoming calls.

3. Click **Diagnose**.
4. Depending on the equipment selected, diagnosis can take several minutes. The System displays the Voice Board Diagnostics results page.
5. If the system displays either of the following messages, the system did not detect a working telephone line connected to the voice port.

   If you see either of the following messages, complete Step a through Step c.

   ```
   No loop current on channel number
   Channel number changed to state FOOS
   ```

   a. Verify that the telephone line is properly connected to both the interface card and the switch.

   b. Verify that the analog line is set up properly on the switch.

   c. Verify that the switch 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 switch is faulty. Verify the wiring and administration of the switch.
      - If the system displays the following message, the system did not detect a dial tone. However, it did detect loop current, which could be a result of excessive load on the analog-line interface card. If you see the following message, complete Steps d and e.

        ```
        Diag TRnumber: No dial tone frequencies set
        ```

   d. Verify that the analog lines are distributed over several analog-line interface cards.

   e. Verify that the switch administration for the ports is valid.

   f. If the system displays either of the following messages, the channel or card is not working and you must replace the analog-line interface card:

      ```
      Channel number changed to state BROKEN
      Card number changed to state BROKEN
      ```

6. If the card is NONEX (nonexistent), verify that the card is properly seated in the slot.

   If the card is not properly seated, correct the seating of the card and then follow the procedures to return power.

Diagnose voice equipment field descriptions

Field Name	Description/Procedure
Equipment to diagnose	Displays the equipment to diagnose as **Card**.
Equipment Number	Specifes the number of the card.
Immediate Diagnosis?	Immediate diagnosis takes specified channels out of service immediately even if a call is in progress. Select **NO** to wait until all specified channels are idle before beginning the diagnosis. **Note:** Selecting **YES** in the Immediate Diagnosis? field disconnects calls in progress. Do not select YES unless call traffic is extremely low. Diagnosing voice cards only when they are free of calls can take longer, but no calls are disconnected.

Displaying voice equipment status

About this task

To display the status of voice equipments:

Procedure

On the Administration menu, click **Messaging** > **Telephony Diagnostics (Application)** > **Display**.
The Display Voice Equipment page appears. For information on the displayed fields, see Display voice equipment status field descriptions on page 212

Display voice equipment status field descriptions

Field Name	Description
Card	Identifies the circuit card on which the channel resides.

Field Name	Description
	For Messaging, this number is always 8.
Port	The virtual port number, 0 through 7.
Channel	The virtual channel number, 0 through 7.
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 and it may have to be replaced
Time	The time and date of the last change in state of the channel.
Service	The associated service name or a DNIS designation indication.
Phone	The switch extensions that correspond to the channel.
Group	Not applicable.
Opts	The equipment options (talk or TDM.)
Type	The type of voice card being used. This column always reads AYC41.

Releasing voice channels

Releasing the voice channels places all channels in service. The 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 appropriate information in the fields.
   For more information, seeRelease voice equipment field descriptions on page 214.
3. Click **Release**.

Result

When the state change is complete, the system displays the Release of Voice Equipment results page.

Release voice equipment field descriptions

Field Name	Description
New State	Specifies the state of the equipment. This field is always **inserv** .
Equipment	This field is always **Channel**.
Equipment Number	Specifes the number of the channel. Enter a valid number or range or all. 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)

Using diagnostic tools

Running application server diagnostics

The Diagnostics (Application) page provides the administrator with the facility to run one or more diagnostics tests to evaluate various components of the application server. For some tests, additional parameters are required to be specified before running the test. All test results display the local time of the client PC where the diagnostics test is being executed.

Procedure

1. Select the test (or all) from the **Select the test(s) to run** drop-down field at the top of the page.

   Depending on the test selected, additional fields are displayed.
2. If additional parameters are required, enter appropriate field value for the associated test to be run.
3. Click **Run Tests**.

Test results (or errors) are displayed in the lower frame. The output results returned are categorized by the diagnostic tests, and the administrator can download the results to a file by clicking Download Results (at the base of the page).

Next steps

You can download the diagnostics logs of all the diagnostics run on the application server from **Messaging** > **Logs** > **Diagnostics Results (Application)**. For more information, see Accessing diagnostics results on page 195

Diagnostics (Application) field descriptions

Diagnostic Test	Description
All tests	Runs all available tests (described in this table). **Note:** At least one MWI extension must be entered (to accommodate the MWI diagnostic test).
Application Distributed Cache	Tests that the distributed cache server is up and running, and checks that data can be read, written, and deleted.
Call-out	Calls out to a specified extension. When the phone is picked up, a test greeting should be heard. Parameters to be specified are: • Telephone Number – The telephone number that the application server calls. • Port Number (optional) – The port (line) that the application server uses to make the call.
Cluster	Tests the application server cluster configuration and connectivity. The test connects to all ADCSs in a cluster to see if they respond.
Communication	Tests the communication facilities of the application server, including the TTS port, the voice browser, the Web server, the messaging application, and the line states. For serial (SMDI/MCI) integrations only, the SMDI or MCI link is also tested.
MWI	Tests the Message Waiting Indicator (MWI) configuration. It will turn the MWI light for the

Diagnostic Test	Description
	extension on and off (a few times) during the test. Parameters to be specified are: • Extension number– Extension number of the user. • MWI port number (optional) – Port number.
User and Contact Lists	Queries the local cache on the application server for a user or contact. Parameters to be specified are: • Type of user/contact list – The contact list that is queried to locate the specified user or contact. Choose from: User List and Global Address List • Mailbox number or email address – The mailbox number or e-mail address of the user or contact to be located.
Voice Messaging Application	Diagnoses the state of the messaging application and its communication link to the AxC.

Testing alarm origination

Use the Test Alarm Origination page to verify that alarms are properly logged and sent to the administered location. Once you run the test on this page, an alarm is raised by the test. If the alarming system uses the modem and you are logged on remotely, log off as soon as possible after running the test.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Diagnostics** > **Alarm Origination**.
   The Test Alarm Origination page appears.
2. To activate the test alarm, click **Run Test**.
   The test alarm becomes active and stays active for 30 minutes after which it retires automatically.

Next steps

To view alarm logs, click **Display**. For more information, see Checking the alarm log on page 182.

Testing LDAP connection

Use Test LDAP Connection to verify that the networked machines are administered correctly. The test attempts to connect to the LDAP server on the selected machine, using the administered IP address, port, name, and password.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Diagnostics** > **LDAP Test Connection**.
2. Select a machine from the drop-down list.
3. Click **Run Test**.

Testing SMTP connection

Use the SMTP connection test to check low level network connectivity. Local or remote service technicians can perform fault isolation of network problems during installation and testing of Internet Messaging.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Diagnostics** > **SMTP Connection**.
   The Internet Messaging: SMTP Connection page appears.
2. Enter the **IP Address or Host Name** of the destination machine to check if the host e-mail system is working
3. Click **Run Test**.

Testing POP3 connection

Use this test to verify check low level network connectivity. Local or remote service technicians can perform fault isolation of network problems during installation and testing of Internet Messaging.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Diagnostics** > **POP3 Connection**.
   The Internet Messaging: POP3 Connection Test page appears.
2. Enter the **IP Address or Host Name** of the destination machine to determine whether the host e-mail system is running.

Testing IMAP4 connection

Use this test to check low level network connectivity. Local or remote service technicians can perform fault isolation of network problems during installation and test of Internet Messaging.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Diagnostics** > **IMAP4 Connection**.
   The Internet Messaging: IMAP4 Connection Test page appears.
2. Enter the **IP Address or Host Name** of the destination to determine whether the host's mail system is running.
3. Click **Run Test**.

Testing mail delivery

Use this test to check high level mail connections. Local or remote service technicians can perform fault isolation of network problems during installation and testing of Internet Messaging.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Diagnostics** > **Mail Delivery**.
   The Internet Messaging: Mail Delivery Test page appears.
2. Enter the sender mailbox extension or e-mail handle in **Sender**.
3. Enter the recipient e-mail address in **Recipient**.
4. click **Run Test**.

Testing Ping Another Server

Use this page to send test packets to the customer LAN or to receive test packets from the customer's LAN. Sending and receiving test packets allows you to verify that the LAN is accessible to the messaging system and to any remote machines on the same LAN. This process also tests the internal setup of the LAN to verify transmissions.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Diagnostics** > **Ping Another Server**.
   The Send and Receive Packets To and From (PING) page appears.
2. Enter the **IP Address/Host Name** from where you want to have test packets sent and returned.
3. Enter the following **Options**:
   a. Enter the number of packets to be transmitted in **Number of ECHO_RESPONSE packets**.
   b. Enter **The size of the packet** to be transmitted.

4. Select the **Do Not Use Hostname Lookup** check box if you do not want to use DNS.
5. Click **Ping Test**.

Testing name server lookup

The Name Server Lookup test determines whether a system can be looked up through the domain name servers assigned on the Network Addressing page. If domains can be looked up, messages can be delivered to those domains. Run the Name Server Lookup test for the Messaging server and the mail gateway.

About this task

Procedure

1. On the Administration menu, click **Messaging** > **Diagnostics** > **Name Server Lookup**.
   The **Test Name Server Lookup** page appears.
2. Enter **Internet host name or IP address** of the system for which you want to run the test.
3. Select a DNS server from the **Select DNS Server** drop-down list.
4. Select the type of information you want to retrieve from the **Record Type** drop-down list.
5. Click **Run Test**.

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 Channel Monitor.

To display the Voice Channel Monitor:

Procedure

1. On the Administration menu, click **Messaging** > **Server Information** > **Voice Channels (Application)**.
2. Enter the new update interval in the **Refresh Rate** field.

The interval can be any interval between 1 and 30 seconds.

3. Click **Display**.

Note:

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

Reload application server cache

The Reload Cache panel allows the administrator to force cache reloads, as required. During normal operations, manual (forced) reloads of the appliance's data caches are not required. However, reloading system caches ensures that what is displayed within the Application server administration interface is synchronized with the Avaya X Connector (AXC) server.

In the following situations, forced operations may be required:

Force a manual reload of **User List**, **Global Address List**, **System Greeting**, or **Classes of service** if there have been network problems that impaired communications between the Avaya X Connector (AXC) and the Application server. For example, cache reloads would be required if changes have been made to extensions associated with local users or caller applications (subsequent to initial creation).

Note:

Reloading the Global Address List is dependent on the size of the list and the responsiveness of the AXC and Active Directory servers. Other cache reloads vary in times, depending on the size.

Force a reload of the System Greeting audio file if it has been updated on the AXC server.

Force a reload of the Classes of Service definition file if this file has been updated on the AXC server.

Force a synchronization of the Distributed Cache whenever the appliance has been offline for a long period of time. The application server synchronizes with the data from the Avaya X Connector (AXC) server to which it is bound.

Viewing AxC address

About this task

The AxC Address page displays the AxC address information such as:

- **AxC IP Address**: IP address of the server where AxC reside.
- **AxC port**: Port with which the AxC is connected.
- **AxC URL base**:

Procedure

On the Administration menu, click **Messaging** > **Advanced** > **AxC Address**.

Verifying the status of the application role

About this task

The Verify System Status (Application/AxC) page displays status of the various processes used for the application role and the connection status with the AxC used by the application role. Status of the following appears on this page:

- Application software release
- System uptime
- AxC IP address
- Time
- Voice Messaging Application
- Last-known AXC status
- Voice Browser
- Text-To-Speech
- Application Distributed Cache Server
- Storage Synchronizer

To access and verify the system status (Application/AxC):

Procedure

Select **Server Information** > **System Status (Application/AxC)**.

Result

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

Monitor cache statistics

Cache server statistics show how cache is being handled in a cluster or single appliance (if no cluster). Statistics are tracked in terms of hit and miss rates in cache appliances and storage usage.

When information is retrieved from the Active Directory and Microsoft Exchange, the data is saved in the appliance cache. If an appliance needs the data again, the cache is queried first, resulting in less requests going back to the Active Directory and Exchange.

In a clustered environment, if the data is not present on the appliance, the appliance queries other appliances for the data before requesting it from Exchange.

Cache statistics are tracked by hit and miss rates and storage usage. Hits represent the data required for the transaction that was found in the cache. Misses represent the data required for the transaction that was not found in the cache. This data is tracked in terms of local counts and cluster-wide counts of voicemails.

- Local cache is the cache on the appliance being viewed. For example, “Voicemail, Local” is the local cache statistics for voicemail elements.
- Cluster cache refers to the collective cache of the cluster (all appliances in the cluster). In the single appliance, local and cluster cache are the same.

  Cluster statistics include statistics based on inbound cache requests from other appliances in the same cluster. Cluster statistics are the same on all appliances in the cluster.

In terms of storage usage, the cache is tracked in terms of local and cluster cache, and storage quota used to support the cache statistics. The **Clear counters** button at the bottom of the Cache Statistics panel is used to clear the cache statistics values.

The following table provides descriptions to the key components of the Cache Hit/Miss Rates panel.

Key	Description
Percentage Values	
L1 hits	Percentage of times a request was made and data was found in the local cache.
L2 hits	Percentage of times that there was a local miss but when another appliance’s cache in the cluster had the data.
Cluster Miss	Percentage of times that the cluster-wide cache had the required data.
Total read attempts	Total times cache was attempted to be read (but may have failed, if there is a value in the **Failed writes** field), reported locally and cluster-wide.

Key	Description
Failed writes	Total times cache was read but failed reported locally and cluster-wide.
Color Bars	
Green	Indicates the cache hits that represent accesses back to Exchange/ Active Directory that were prevented by the cache technology.
Yellow	Indicates that the cache worked, but that the cluster cache was leveraged instead of the local cache.
Red	Indicates cache misses, resulting in access back to Exchange/Active Directory.

Enabling core file generation

Use this page to specify core file generation details for the Messaging system. Depending on the specifications here, core files are created when the Messaging program terminates unexpectedly due to a bug. These core files can help figure out what went wrong. It contains a detailed description of the state that the program was in when it terminated.

Procedure

1. On the Administration menu, click **Messaging** > **Advanced** > **Core Files**.
2. For **Core File Generation**, select one of the following:
   - To enable core file generation, select **enabled**.
   - To disable core file generation, select **disabled**.
3. Enter **Max Core File Size**.
4. Enter **Max Cores Per Application**.
5. Click **Apply**.

Verifying or restarting the LDAP processes

The LDAP Status/Restart page displays the current status of the LDAP processes and allows LDAPFE and LDAPCORP to be manually restarted. LDAPFE and LDAPCORP are used to administer the Messaging data from internal and external client respectively.

Procedure

1. On the Administration menu, click **Messaging** > **Utilities** > **LDAP Status/Restart (Storage)**.
2. Verify if all the processes are up.
3. If any process is not up, click **Restart** to manually start the process.

Note:
To start all the LDAP processes, you must restart the Messaging application.

Verify LDAP processes field descriptions

Field Name	Description
slapd	slapd is the core process for LDAP in Messaging. Messaging functions only when slapd is running. To restart slapd, you must bring Messaging system down. UP Indicates that slapd is running normally. DOWN Indicates that slapd is not running. Messaging is not functioning correctly and should be restarted as a whole. Refer to the Stop Messaging and Start Messaging pages.
Ldapfe	Ldapfe is the process to perform administration from the Web pages. UP Indicates that Ldapfe is running normally. DOWN Indicates that Ldapfe is not running. Administration through the Web pages cannot be performed until this process has been restarted.
Ldapcorp	Ldapcorp is the process to perform administration from the external LDAP clients. The firewall must also be open to perform administration through external clients. Refer to the page **Server (Maintenance)** > **Security** > **firewall**. UP Indicates that Ldapcorp is running normally. DOWN Indicates that Ldapcorp is not running. Administration through the external LDAP clients cannot be performed until this process has been restarted.

Server maintenance

Process Status

Purpose

Use the Process Status Web page to view status information of server applications. Each application is a collection of processes. You can view information about each entire application or its individual processes. You can also choose whether you want a static display or a periodically refreshed status information.

Content

- **Summary**. This default option provides information about each server application as a whole, including a count of the application processes running 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**. This 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**. This default option displays the status results once in the Process Status results page. The page is not refreshed even when the status changes.
- **Refresh page every __ seconds**. This option displays the status results every few seconds, based on the value you select from the drop-down list.

Note:

These settings apply to both the summary and detailed displays.

View process status

Click **View** to display the process status for all the server applications.

View Process Status Results

Purpose

This Web page displays status information for the server applications based on the selection you made on theProcess Status on page 226 page: Summary or Detailed.

Application status information

Regardless of which view you chose, status information appears for the following applications:

Application Name	Description
Watchdog	Brings the system up, recovers from failures, and brings the system down cleanly.
TraceLogger	Creates and maintains the log files where most Avaya Call Processing (telephony application) applications write messages.
ENV (environment)	Monitors the environmental variables of the physical hardware, such as temperature, voltage, and fan speed.
LicenseServer	Provides security for enabling the different software features, including the ability to run telephony application .
INADSAlarmAgent	Sends alarms to the Initialization and Administration System (INADS) using SNMP traps defined in the INADS Management Information Base (MIB).
G3AlarmAgent	Reports alarms using Simple Network Management Protocol (SNMP) traps defined in the G3 MIB.
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.
arbiter	Decides which server should be “active” running the telephony application software, based on the state-of-health information from the other components.
filesyncd	Manages file synchronization between the servers so that critical files such as translations are kept up to date.
dupmgr	Replicates information between the servers to allow arbitration between the servers with minimal interference with call processing.
MasterAgent	Is a gateway SNMP agent for the server. The MasterAgent receives all SNMP requests (both reads and writes) to the server. It also validates that a requester can access the requested objects, and it calls on a specific subagent to process the request.
MIB2agent	Handles SNMP requests for objects defined in the MIB-2.
MVSubagent	Process that provides SNMP access to MV configuration fault and performance data.
SME (Server Maintenance Engine)	Tests server components periodically. The SME tests components as the result of both specific requests and asynchronous errors.

Application Name	Description
Communication Manager	Controls the communications sessions and features.

Process status summary format

The system default for displaying process status information is a summary display. The summary display looks something like this:

Watchdog	16/16	UP
TraceLogger	3	Partially Up
ENV	0/1	DOWN

In this example, you can see the following information:

- Name of the application (Watchdog).
- Number of processes running compared to the total number of processes associated with the application (16/16).
- Application status (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 as a whole. However, it also displays information about each process associated with an application. The detailed display looks something like this:

```
Communication Manager 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:

- Name of the application (Communication Manager).
- Number of processes running compared to the total number of processes associated with the application (58/85).
- Application status (PARTIALLY UP). The application status is either up, partially up, or down.
- List of processes associated with the application. The process list shows the truncated process name, followed by a plus or minus sign (for example, ps_mapm+ and isg-). The plus sign indicates that the process is running; 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 copies running compared to the number expected (for example, prc_mgr [3/3].

Shut down Server

Purpose

Use the Shutdown Server page to shut down the server immediately or later. You can also configure the server settings to restart the server after the shutdown.

Note:

When you shut down this server, the Web server stops running all the processes. You can not access the Web pages until the system starts.

Delayed shutdown

When you select this default option, the system notifies all processes that the server will be shut down. The system waits for the processes to close files and perform other clean-up activities before it shuts the server down.

Immediate shutdown

When you select this option, the system does not wait for processes that are running to terminate before it shuts the server down. Data may be lost.

Restart server after shutdown

Select this option to restart the system after shutting down.

When you shut down a server, the system displays one of the following messages on the results page. The displayed message depends on the conditions under which you attempted to shut down the server. Possible results message include:

```
shutdownproc accepted.Global shutdown is now in progress.
```

If you chose to do a delayed shutdown of the server, you will see this message when the system successfully begins the shutdown.

No message

If you chose to shut down the server immediately, the results page will be blank because all contact to the server is lost when it is shut down.

Ping

Purpose

Use the Ping page to execute the ping command for information about your network. Typically, use the ping command to:

- Test whether or not 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.

Endpoints to Ping

You can run the ping command to verify any one of the following endpoints at a time:

- **Host Name Or IP address**: Select this option and enter the host name or IP address you want to ping.
  - **IPv4**: Select this option if the system has IPv4 connectivity. By default, this option is selected.
  - **IPv6**: Select this option if the system has IPv6 connectivity. This option is displayed only if the system has IPv6 connectivity.

    Important:

    The IPv6 Address field is limited to a specific customer set and not for general use.

    Note:

    If you have made an entry in the **Host Name or IP Address** field, you must select either **IPv4** or **IPv6**, or both. When you select both **IPv4** and **IPv6** and run the **`ping`**

command, the Execute Ping results page shows the ping results for both networks.

- **IPSI's with cab number (1~99) ____ carrier number____**: Select this option to verify the IPSI connectivity. Enter the cab number and select the carrier number.
- **Other server via duplication link**: Select this option to verify network connectivity to the duplicated server through a duplication link.

Options

- **Do not look up symbolic names for host addresses**: Select this option to ping the server by using an IP address. If you do not select this option, 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. The ping command fails if the domain name server is unavailable.
- **Bypass normal routing tables and send directly to a host**: Select this option to ping a local host on an attached network. That is, select this option to bypass the routing table and ping a local host through an interface that has no route through it.

  If the host is not on a network that is directly attached, the ping is unsuccessful and the system displays an error message.
- **Use alternate interface ____ as the source**: This field appears only if you have selected **IPv6** under **Host Name Or IP Address**. Select an alternate Ethernet interface as the source from the list.

  The system uses the selected interface to execute the **`ping`** command.

Execute Ping

Click **Execute Ping** to start the ping command. If the ping is successful, the Execute Ping results page displays a brief summary that shows the number of packets sent and received. The summary also shows the minimum, average, and maximum of the round-trip times.

Ping results

When you run the ping on page 230 command, a Web page appears to show whether the command was successful or not. The following sections describe successful and unsuccessful ping results:

Successful ping results

If the ping command runs successfully, the Execute Ping results page displays a brief summary that looks something like this:

```
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 Execute Ping results page displays an error message. Each error message points to one or more possible problems, as follows:

`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 there is a problem with the network so that the ping packets cannot reach the host.

Traceroute

Purpose

You can use this 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 connecting the Avaya server network hardware. To trace the IP packet route, the **traceroute** command launches probe packets with a small time to live in the connection path and then listens for a time exceeded reply from a gateway.

You can use the **traceroute** command to evaluate the hops taken between the links in your TCP/IP network. Hops are the short, individual trips that packets take from one router to another on the way to their destinations.

Host Name or IP Address

In the **Host Name or IP Address** field, you must select either `IPv4` or `IPv6`, or both. If you select both `IPv4` and `IPv6` and run the **traceroute** command, the Execute Traceroute Results page displays whether the command was successful for both the networks.

- **IPv4**: Select this option , if the system has IPv4 connectivity. If you select `IPv4` , a new field **Use alternate IPv4 address** ____ **as the source address** appears under **Options** in the Traceroute page. By default, this field is selected.
- **IPv6** : Select this option, if the system has IPv6 connectivity. This option is displayed only if the system has IPv6 connectivity. If you select `IPv6`, a new field **Use alternate interface** ____ **as the source** appears under **Options** in the Traceroute page.

Important:

The IPv6 Address field is limited to a specific customer set and not for general use.

Options

Print address numerically	Select this option to print the hop addresses numerically rather than by symbolic name and number. If you do not select this option, 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.
Bypass routing tables and send directly to host	Select this option to run the **`traceroute`** to a local host through an interface that has no route through it. That is, select this option to run the **`traceroute`** to a local host on an attached network. If the host is not on a network that is directly attached, the **`traceroute`** is unsuccessful and the system displays an error message.
Use alternate IPv4 address ____ as the source address	This field appears only if you have selected `IPv4` under **Host Name or IP Address**. Select an alternate IPv4 address as the source address from the list.
Use alternate interface ____ as the source	This field appears only if you have selected `IPv6` under **Host Name or IP Address**. Select an alternate Ethernet interface as the source from the list. The system uses the selected interface to execute the **`traceroute`** command.

To execute

Click **Execute Traceroute** to view the connection path.

Traceroute Results

When youTraceroute on page 232 command, the Execute Traceroute results page shows whether the command was successful or not. The following sections describe successful and unsuccessful traceroute results.

Successful traceroute results

If the traceroute command runs successfully, the Execute Traceroute results page displays a summary that looks something like this:

```
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 given above, the traceroute output in the first line differs from the output in subsequent lines. The following two sections describe the traceroute output:

First line of output

The first line of traceroute output describes the parameters within which the command was run.

It shows:

- 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 show:

- 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 elected to print the addresses numerically, no host name appears 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, it indicates a hop has exceeded some limit.

Unsuccessful traceroute results

If the traceroute command does not run successfully, the Execute Traceroute results 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

Purpose

Use this Netstat 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.

Output type

- **View the status of network connections by listing the open sockets [default]**: Select this option to view the active Internet connections, except those associated with the server processes. By default, this option is selected.
- **View all sockets**: Select this option to view the state of all domain sockets, including those used by server processes.
- **View listening sockets only**: Select this option to view only those active domain sockets that are used by server processes.
- **Display routing table**: Select this option to view the routing table for specific IP addresses.
- **Display networking interfaces**: Select this option to view the kernel interface table, which provides information about the packet traffic on the network interfaces.

Output format

To ensure that the addresses display numerically on the results page, select **Show Numeric Addresses**.

Note:

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 will be unsuccessful.

Show only the following address families

- **inet**: Select this option 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**: Select this option to view the IPv6 routing table entries.
- **unix**: Select this option to limit the statistics or address control block reports to UNIX addresses. The socket type is AF_UNIX; that is, local machine socket.

Note:

To view results for inet, inet6, and UNIX address families on the same page, select all the options.

To Execute

Click **Execute Netstat** to obtain information about server conditions.

Netstat results

Purpose

The information displayed in the Netstat results page depends on your output type selection using the Execute Netstat on page 234 command. The sample results below combine output for inet and UNIX address families and *may not be applicable to each output type selection*.

The sample result given above shows output for both inet and UNIX address families. 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/

Proto is the protocol used by the socket.

Recv-Q is the number of bytes not copied by the user program connected to the socket.

Send-Q is the number of bytes not acknowledged by the remote host.

Local Address is the host name of the socket.

Foreign Address is the remote host name and port number of the socket.

State is 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.

CLOSED The socket is not being used.

CLOSE_WAIT The remote end has shut down, and it 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	

Proto	Is the protocol used by the socket.
RefCnt	Is the reference count of processes attached via this socket.
Flags	Is used for unconnected sockets if their corresponding processes are waiting for a connect request.
Type	Is the type of socket access, as follows:
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 serves reliably delivered messages.
SOCK_SEQPACKET	The socket is a sequential packet socket.
SOCK_PACKET RAW	The socket is an interface access socket.
UNKNOWN	The socket is unknown.
State	Is the state of the socket. For a list of possible socket states, see the description for inet address families.
I-Node	Is the associated file for this socket, shown as an I-node number.
Path	Is the path name of the processes attached to the socket.

Add Access Mask

About this task

This page allows you to specify a new access mask. Enter the new access mask number and select how the mask should be created. There are three options for creating a mask:

- Create by copying from an existing access mask number.
- Create and set all values to enable access.
- Create and set all vales to disable access.

Procedure

Click **Submit** to add the access mask.

Change Access Mask

About this task

The Change Access Mask page allows for changing access mask names and permissions to menu items (Web pages). These menu items are listed by category and will be shown in the left navigation pane for the user. Menu items with check marks will be accessible for that particular access mask.

Procedure

Make the appropriate changes then click **Submit**.

Delete Access Mask

About this task

This page allows deletion of an existing access mask. The properties for the access mask you selected on the Web Access Mask page is displayed.

Procedure

1. Verify the access mask is the one you want deleted, then click **Submit** to delete.
2. If the access mask is not the one you want deleted, click the browser back button and enter the appropriate access mask number.

Web Access Mask

Purpose

use the Web Access Mask page to further 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 affect Communication Manager access also.

Access masks and names

There are two types of access masks, default and user-defined. Default fixed masks are 0-17, 18 and 19 and may not be edited. User-defined access masks and names may be modified by the user. Default access masks are:

Mask	Name
0-17	System profiles
18	Customer Super User
19	Customer Non-Super User

You may 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 for modifying masks:

Add Click **Add** to add a new mask. The Add Access Mask page is displayed.

Change Click **Change** to modify the existing access masks.

Delete Click **Delete** to remove an existing mask. The Delete Access Mask page is displayed.

View Selected Click **View Selected** to view properties of the selected access masks .

View All Click **View All** to view properties of all the user-defined access masks.

Select All Click **Select All** to select all user-defined access masks listed on the page.

De-Select All Click **De-Select All** to de-select all user-defined access masks listed on the page.

Filesync Click **Filesync** to update the LSP and/or ESS servers on a duplicated system, after you have added, changed or deleted profiles.

View access mask and view all access masks

The View Access Mask and View All Access Masks pages show the Web menu items (Web pages) accessible for each user profile. These menu items are listed by category and will be shown in the left navigation pane for the user. Menu items with check marks will be accessible for that particular access mask.

Trusted Certificates

The Trusted Certificates page enables you to manage the trusted certificate repositories for the server. The Trusted Certificates page displays all the installed certificates. Use this page to install a certificate, copy an existing certificate to other repositories, or remove a certificate from repositories.

The Trusted Certificates page displays the following content of the trusted certificates:

- **File**: The **File** column shows the file name of the certificates individual file, which is the same in all repositories.
- **Issued To**: The **Issued To** column displays the name of the company to whom the certificate is issued.
- **Issued By**: The **Issued By** column displays the name of the company who has issued the certificate.
- **Expiration Date**: The **Expiration Date** column displays the date of the certificate expiration.
- **Trusted By**: The **Trusted By** column displays the list of single letter identifiers for the repositories in which the certificate is installed.

Displaying a certificate:

1. Select a certificate entry.
2. Click **Display** to display the content of the selected certificate.

   The Trusted Certificates - Display page displays the content of the selected certificate.

Adding a trusted certificate:

A trusted certificate must be a Certificate Authority (CA) certificate.

1. Click **Add** to add a certificate to the server. The system displays the Trusted Certificates – Add page.
2. Enter the file name of a certificate to add. The certificate, which you want to add, must be in a `pem` file and must be in the `/var/home/ftp/pub` directory.
3. Click **Open** to validate the certificate.

After successful verification, the Trusted Certificates – Add page shows the issued-to, issued by, and date of expiration information for the certificate to be added.

Note:

If the file does not contain a valid certificate, the system displays an error message instead of the certificate content.

4. Enter a file name to use to store the certificate (same name in each repository).
5. Select the appropriate repositories check box in which the certificate need to be installed.
6. Click **Add**.

   The system verifies the following:

   a. If the file name does not end with a `crt` extension, the system deletes the entered extension and replaces with a `crt` extension prior to creating the file.

   b. The Web page verifies if the file name is unique and does not already exist.

   c. The Web page verifies if a certificate is not duplicated using a new file name.

Note:

If you fail to install a certificate in one repository, it does not affect the installation in other repositories.

Removing a certificate:

1. Select a certificate entry.
2. Click **Remove** to delete the certificate.

   The Trusted Certificates – Remove page shows the file name, issued-to, issued by, date of expiration, and trusted-by information for the selected certificate.
3. Select the appropriate checkbox to remove the certificate from a single repository or from an arbitrary combination of repositories if it is installed in more than one.
4. Click **Remove**.

Copying a certificate:

1. Select a certificate entry.
2. Click **Copy**. The Trusted Certificates – Copy page shows the certificate content along with a list of all the other repositories from which you can select in any combination.

3. Select the repositories check box in which you want to install the selected certificate.
4. Click **Copy** to install the selected certificate in the selected repositories.

   The system verifies the following:

   a. The Web page verifies if the file name is unique and does not already exist.

   b. The Web page verifies if a certificate is not duplicated using a new file name.

Note:

If you fail to install a certificate in one repository, it does not affect the installation in other repositories.