Avaya Aura® Messaging Overview and Planning

6.1
CID: 151125
June 2012

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, Octel, 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.

Contents

Chapter 1: Avaya Aura® Messaging overview

Avaya Aura® Messaging, also referred to as Messaging, is the latest messaging product from Avaya.

Messaging is flexible, scalable, resilient and easy to deploy on standard Linux-based servers. Messaging is an enterprise-class messaging system targeted at flexible deployment options in single site and multisite environments.

Messaging enhances productivity by enabling quick and effective communication and collaboration across an enterprise. Using the variety of features and capabilities the solution offers, end users can receive and respond to calls and contacts from customers, partners, and coworkers faster and more efficiently.

Note:

A user is a person who has an account on the Messaging system. Any person who calls into the Messaging system is a caller.

Messaging can improve your business by enabling employees to work more effectively and make better decisions while lowering acquisition and operating costs, with unique and powerful messaging capabilities that deliver tangible benefits:

- Allowing important calls to get to the right person, at the right time.
- Alerting employees to critical new messages.
- Providing fast and easy access to all messages.
- Lowering the cost of acquisition, implementation, and ownership of the Messaging systems through standards-based interfaces that allow easy integration with the existing networks, administrative systems, and security processes.
- Providing multiple configuration choices for scalability to enable system consolidation, significantly lowering total cost of ownership (TCO) while offering new business continuity options.

Benefits of Messaging

The core strengths of Messaging are compatibility, interoperability, scalability, and resilience, combined with flexibility and easy availability. Together, these features improve how your organization responds to customers, enhances collaboration, and lowers the cost of ownership.

Messaging provides the following benefits to customers:

- Flexibility: Messaging offers a flexible architecture designed to fit a wide variety of customer environments and is ideal for enterprises with telephony environments that are in transition. Depending on how the system administrator configures Messaging, users can have their voice messages on the Avaya message store, the Microsoft Exchange message store, or the VMware Zimbra message store.
- Compatibility: Messaging fits into your infrastructure so you do not have to replace or update existing networks, administrative systems, or standards-based interfaces, thereby lowering the total cost of ownership.
- Scalability: Messaging provides a scalable solution that ranges from an easy-to-deploy single server to a fully scalable multiserver configuration with dedicated application and storage servers.
- Resilience: Messaging delivers high availability and disaster recovery options ranging from a cluster configuration of redundant application servers to locally survivable application servers.
- Remote alarming and serviceability: Messaging uses Secure Access Link (SAL) 1.5 to provide remote alarming and serviceability.
- Interoperability: Messaging interoperates with several Avaya products as well as various third-party products like AudioCodes gateways and third-party fax solutions.
- Multilingual support: All end-user features are available in multiple languages.
- End-user features: Users can use Messaging to combine notification features, such as MWI, Reach Me, and Notify Me. Messaging also offers voice recognition for addressing messages, access to voice messages using an Internet Message Access Protocol 4 (IMAP4) e-mail client, a clientless e-mail toolbar, a browser application for managing user settings, and text conversion of voice messages (requires a third-party solution).

Accessibility and mobility

A key component of business agility is the ability to contact the right person at the right time and the right person might be another employee or your customer. To facilitate this agility, organizations are investing in mobile devices using which users can become more mobile and accessible than before.

Messaging can improve communication by connecting users, enabling users to collaborate efficiently, and by streamlining business processes. Users can access their messages over a telephone using the TUI, Avaya one-X® Speech, or an IMAP4 based e-mail client such as Microsoft Outlook and Zimbra. Users can access their messages using a smartphone that has access to the Exchange or Zimbra message store.

One-number connectivity

Your business telephone number is a part of your corporate identity. When you enable Reach Me, Messaging preserves that business number as Messaging routes callers to your cell

phone, your remote office, or your virtual office. Irrespective of the access method you use, one-number connectivity preserves your corporate identity.

Flexibility

Messaging works in a wide variety of topologies in centralized and distributed environments.

The flexible architecture of Messaging is designed to fit a wide variety of customer environments. Messaging is a scalable solution ranging from an easy-to-deploy single server with application and storage roles combined on a single virtual machine to a fully scalable multi-server configuration with dedicated application and storage servers.

Compatibility

Messaging is compatible with the existing infrastructure of the customers. Messaging is cost-effective as customers are not required to replace everything in the network.

Messaging is compatible with:

- Internet Browsers: Microsoft Internet Explorer 7.0 and 8.0, Mozilla Firefox v3.5, or Safari v4.
- Messaging toolbar support for Microsoft Outlook 2003, 2007, and 2010, and VMware Zimbra Web client.
- IMAP4 based e-mail clients.

Industry standards

Messaging supports the following industry standards:

- IMAP4 client access to messages
- SMTP/MIME for sending and receiving messages
- Session Initiation Protocol (SIP)

Flexible storage

With the Messaging flexible storage capability, you can use multiple storage destinations. The supported storage destinations include the following:

- Avaya message store
- Microsoft Exchange (Exchange 2007 and Exchange 2010)
- VMware Zimbra 7.0.1 (on-premises only)

After the administrator configures the storage destinations in the Messaging system, you can use any one of the configured storage destinations.

Scalability

The Messaging architecture achieves high scalability as Messaging fits and grows with various telephony deployment sizes, ranging from small branch office telephony servers to larger campus-wide telephony servers. Messaging is designed to work with large-scale installations over large, global IP networks with varying levels of network quality. For example, in a scalable deployment of the Messaging system, multiple sites can contain multiple application servers, connected to a dedicated storage server.

For further scalability, individual Messaging systems can be combined into a single voice mail network using standard voice mail networking, either directly (point-to-point) or using Message Networking.

Resilience

The Messaging solution is very resilient as Messaging can remain functional even with major network or hardware failures.

Redundancy

Messaging architecture provides a range of high availability and disaster recovery (HA/DR) options that range from an N+1 configuration for application servers to locally survivable application servers that can stay fully operational with locally cached messages and directory information, including greetings, recorded names, and relevant setting.

For more information, see Redundancy on page 53.

Local survivability

Each application server can operate in the offline mode, thereby providing local survivability in case your data network fails and the application server loses connectivity with the storage server. The offline handling of messages and directory information means that Messaging can continue to provide call-answering service, basic message review, and voice messaging capability.

Offline handling in the Messaging system is session-based and only applies to those users who are affected by the outages in the data network. For example, if the application server connects to more than one storage server and only loses connectivity to one of the storage server, offline handling applies only to the users of the storage server that is offline. Service for users with storage on the operational storage server is unaffected.

The Messaging system is capable of handling local outages because the application server maintains a cache of relevant data, such as:

- Directory information (including greetings, recorded names, and relevant setting)
- Voice messages

The cache is a hybrid or distributed cache. Directory data is cached on a single application server. Voice messages are stored in a cache that is distributed among the application servers in a cluster.

In an offline mode, users can still use the TUI and access messages that were received in the past three days or as configured. Users can also access any new messages received after the outage began. For information about the features that are temporarily unavailable, see Limitations of local survivability on page 55.

Disaster recovery

You can provide disaster recovery capabilities for your Messaging system when you configure a cluster of application severs over a WAN. For example, when your IP-based telephony servers are distributed over two geographical locations and connected by a WAN, you can configure your Messaging cluster so that some of the application servers are co-located with each telephony server. For more information, see Clustering on page 48.

Remote alarming and serviceability

Messaging uses Secure Access Link (SAL) and SNMP to provide remote alarming and serviceability.

Secure Access Link

System Platform includes SAL gateway to manage service delivery, including alarming and remote access. SAL gateway is a software application that:

- Facilitates remote access to support personnel and tools that are needed to access supported devices
- Collects and sends alarm information to a Secure Access Concentrator Core Server on behalf of the managed devices
- Provides a UI to configure its interfaces to managed devices, Concentrator Remote and Core Servers, and other settings

SAL requires a customer-to-Avaya upload bandwidth of at least 90 KBps (720 Kbps), with a round-trip latency less than 150 ms.

During the installation of System Platform, you must register the system, which consists of System Platform, the solution templates, and SAL gateway, and configure SAL for the customer network.

Important:

For Avaya to provide support, Avaya Partners or their customers must ensure that SAL is registered and configured properly. Avaya support will be delayed or not possible if SAL is not properly implemented.

To deliver remote services, Avaya Partners must provide their own business-to-business connection, which may be a virtual private network or other IP-based connectivity.

Administrators can launch the SAL gateway management portal from within System Platform.

SNMP

The application server and storage server can also use SNMP to send the alarm notifications to a customer Network Management Station (NMS).

The storage server provides support for SNMP GET requests. The application server does not provide support for SNMP GET requests. The application server and the storage server do not provide support for SNMP SET requests.

Interoperability

The key benefits of Messaging include interoperability with several Avaya Aura® products. Messaging also provides interoperability with various third-party products including AudioCodes gateways and third-party fax servers.

Interoperability with Avaya products

Messaging interoperates with the Avaya Aura® solution, which is a rich, highly interoperable set of SIP components. Messaging interoperates with:

- Avaya Aura® Session Manager: A SIP routing and integration tool that integrates all SIP entities across the entire enterprise network within an organization.
- Avaya Aura® Communication Manager: Provides SIP connectivity.
- Avaya CS1000: Provides SIP connectivity.
- SIP Enablement Services proxy: Provides a smooth migration path into SIP-based communications with support for SIP trunking.
- Avaya one-X® Speech: Provides speech access and voice control of e-mail and voice mail messages.

- Message Networking: To network with traditional voice messaging systems, and also used to provide hub and spoke networking to reduce network administration and to act as a directory concentrator for all messaging systems.
- ProVision: A provisioning tool used to collect user information for the Messaging system. ProVision sends the collected data to the storage server through an LDAP connection.

For more information on the supported versions of the Avaya products, see Supported versions of Avaya products on page 73.

Interoperability with Avaya CS1000

Messaging Release 6.0 supported the switch integration to Avaya CS1000 only through an AudioCodes SIP gateway. Messaging Release 6.1 provides improved integration capabilities, as listed in the following table:

Use	CS1000 R6.0	CS1000 R7.0	CS1000 R7.5
AudioCodes SIP gateway	Yes	Yes	Yes
Session Manager including SRTP	No	No	No
Session Manager without SRTP	No	No	Yes, through SM 6.1
SES	No	No	No
Direct (without Session Manager), Single application server for a single telephony server integration, no SRTP, no TLS	Yes	No	No
Direct (without Session Manager), Single application server for a single telephony server integration, including SRTP	No	No	No
Direct, multiple application servers for a single telephony server integration	No	No	No

Interoperability with third-party products

Messaging interoperates with the following third-party products:

- Storage destinations
- AudioCodes gateways
- Fax servers

Storage destinations

Messaging supports Microsoft Exchange 2007 and Microsoft Exchange 2010. Messaging does not support Exchange Online or Microsoft Exchange 2003.

Messaging supports on-premises VMware Zimbra Collaboration Server (ZCS) 7.0.1 as the message store.

AudioCodes gateways

Messaging uses SIP for integration with mixed telephony server environments. An AudioCodes Mediant 1000 gateway allows the Messaging system to work with telephony servers that are not supported by SIP Enablement Services and Session Manager, mainly telephony servers from third-party vendors.

Additional documentation for AudioCodes gateways and the supported telephony servers is available at http://www.audiocodes.com/support.

Third-party fax servers

Using Messaging, you can receive incoming faxes using the native fax and third-party fax methods. For third-party fax support, Messaging requires that a third-party fax server be installed and configured. Often, an organization already has a fax server installed that can integrate with the Messaging system. Instructions to install and configure the fax server are specific to the particular brand of fax server.

Multilingual support

Messaging supports the following languages for this release, depending on the language packs that you install:

- Brazilian Portuguese
- Canadian French with French GUI
- English (U.K.) with English (U.S.) GUI
- English (U.S.)
- French
- German
- Italian
- Japanese
- Korean
- Latin American Spanish
- Russian
- Chinese (Simplified)

Note:

GUI includes User Preferences, Outlook forms, and online help for User Preferences and Outlook forms.

For more information, see Language packs on page 63.

What's New in Avaya Aura® Messaging 6.1

Avaya Aura® Messaging Release 6.1 offers new features and functionalities that extend the product capability and enhance the user experience.

Flexible storage destinations

Messaging supports three storage destination options for voice mail. You can store voice mail on the Avaya storage server, on a Microsoft Exchange storage server, or on a VMware Zimbra storage server. Storage destinations are not mutually exclusive, enabling administrators to set up some users on one storage destination and other users on a different storage destination.

Microsoft Exchange message store support

Messaging supports Microsoft Exchange 2007 and Microsoft Exchange 2010. Messaging does not support Exchange Online or Microsoft Exchange 2003.

Messaging also supports Active Directory provisioning, lowering the cost of ownership by making it easier for administrators to add users.

VMware Zimbra message store support

Messaging supports on-premises VMware Zimbra Collaboration Server (ZCS) 7.0.1 as the message store. Messaging does not support off-premises VMware Zimbra.

Full E.164 Dial Plan support

Administrators can configure numbers with fewer digits and map them to full E.164 numbers, enabling users at local sites to continue to use mailbox numbers that are shorter but still uniquely identifiable.

For more information, see E.164 Dial Plan on page 67.

Mainstream and Basic mailbox licensing

Messaging offers two mailbox licenses: Mainstream and Basic. The Mainstream license provides the full featured Messaging system that includes the features that are not available in the basic license, including Reach Me, Notify Me, and speech based addressing features, plus fax support and IMAP access to the Avaya message store. The Basic license provides traditional call answering and voice messaging functionality. The Basic license also provides the flexible storage destinations option and the User Preferences Web pages.

Administrators can mix Mainstream and Basic licenses on a single system.

Interoperability with Avaya CS1000

Messaging Release 6.0 supported integration to the Avaya CS1000 only through an AudioCodes SIP gateway. Messaging now provides improved integration capabilities, through Session Manager. For more information, see Interoperability with Avaya CS1000 on page 15.

Multiple server support

Messaging supports the following Avaya-provided hardware platforms for new installations of the system software:

- Dell™ PowerEdge™ R610 Server
- HP ProLiant DL360 G7 Server
- S8800 Server
- S8730 Server

For more information, see Supported hardware on page 42.

Audix TUI support

Messaging Release 6.0 solution supported only the Aria TUI. Messaging 6.1 introduces support for an Audix TUI. The Audix TUI experience is similar to that of an Intuity Audix. The most commonly used commands are available with the same key command sequences so that users of Intuity Audix and Communication Manager Messaging do not need to be retrained.

Fax handling

In addition to detecting and transferring to a third part fax server, Messaging now supports a native fax capability that receives and forwards faxes to a specified e-mail address. Callers can send faxes directly to your DID or extension.

Data migration from Intuity Audix

Organizations that are upgrading from Intuity Audix R5.1 can preserve the following user data through the Avaya ProVision migration tool:

- Voice mail messages
- Recorded names and greetings
- Basic mailbox information
- User options data, including:
  - Personal attendant/assistant extension
  - Time zone
  - Language preference
  - Message playback order

For information about migrating from Intuity Audix, contact Avaya Professional Services or your Avaya Business Partner.

Enhanced security to restrict callers from reaching the system main menu

Administrators can restrict callers from exiting to the main menu after leaving a message for a user using the Aria TUI. Activating this security feature blocks the ability of callers to press

*, #, or 2 to gain access to the system main menu, from where other mailboxes can be reached.

On a Messaging system with multiple application servers, the administrator must activate the restrictions of caller access to the system main menu on each application server using the System parameters page in SMI. If the application server on which these restrictions are activated is in a cluster, then the administrator must activate these restrictions on each application server in the cluster.

Messaging documentation

You can download the document you need from the Avaya Support Web site at https://support.avaya.com/css/Products/P0792.

The following table lists all the documents pertaining to Messaging:

Title	Description	Audience
Planning		
Avaya Aura® Messaging Overview and Planning	Contains information on the concepts underlying Messaging. Topics include features, components, addressing, telephony, deployment options, and planning data.	All
Avaya Aura® Messaging Security Design	Discusses the multilayer security philosophy of Avaya, network security integration, and toll fraud security resources. Elaborates on the security issues that customers must consider before designing and implementing a corporate security strategy into the Avaya enterprise. Also provides recommendations on maintaining and monitoring security in an Avaya enterprise.	Planner, Administrator, Technician
Installation		
Implementing Avaya Aura® Messaging	Provides procedures to install Messaging. Topics include installing System Platform, Messaging, and patches. Also contains Secure Access Link configuration procedures, installation prerequisites, planning forms, and checklists.	Technician
Upgrading Avaya Aura® Messaging	Explains procedures for upgrading Messaging from Releases 6.0 or Release	Technician

Title	Description	Audience
	6.0.1 to Release 6.1 for single-server and multiserver configuration.	
Installing the Dell™ PowerEdge™ R610 Server	Describes the components, specifications, and configurations of the Dell™ PowerEdge™ R610 server.	Technician
Installing the HP DL360 G7 Server	Describes the components, specifications, and configurations of the HP DL360 G7 server.	Technician
Maintenance		
Maintaining the Avaya S8800 1U Server for Avaya Aura® Messaging	Illustrates S8800 support for Messaging. Also describes the procedure required for multiple maintenance tasks for the S8800 1U model.	Technician
Maintaining and Troubleshooting the Dell™ PowerEdge™ R610 Server	Describes how to add, replace, or repair the Dell™ PowerEdge™ R610 hardware components. Also provides information about LCD status messages.	Technician
Maintaining and Troubleshooting the HP ProLiant DL360 G7 Server	Describes how to add, replace, or repair the HP DL360 G7 hardware components.	Technician
Administration		
Administering Avaya Aura® Messaging	Describes the administration of the Messaging system. Provides information about administering Messaging, administering server, managing software, and using diagnostic tools.	Administrator
Help for Administrators	Contains online help topics that explain the procedures to administer the application server and the storage server.	Administrator
Job aid for Administering Avaya Aura® Messaging	Provides common day-to-day administration procedures for Messaging. The topics include reboot procedures, checking application and storage alarms, adding and deleting mailboxes, getting performance indicators, and unlocking, resetting, and changing mailbox passwords.	Administrator
End user		

Title	Description	Audience
Using Avaya Aura® Messaging	Describes common end-user tasks, such as initial setup and using the User Preferences and Messaging toolbar.	User
Avaya Aura® Messaging Quick Reference (Aria)	Describes how to perform common tasks and use Messaging features through the Aria telephone user interface.	User
Avaya Aura® Messaging Quick Reference (AUDIX)	Describes how to perform common tasks and use Messaging features through the AUDIX telephone user interface.	User
Using Avaya Aura® Messaging Online Help	Explains the common end-user tasks, such as initial setup and using the User Preferences and Messaging toolbar.	User
Additional resources		
Documentation library	Provides the entire documentation set for Messaging that includes administration, implementation, general reference, and user information.	All

Chapter 2: User features

Avaya Aura® Messaging provides a range of options for sending, receiving, and managing voice messages. The feature set available to individual users is controlled by licensing and Class of Service definitions. You can interact with Messaging through the traditional telephone user interface (TUI) from any phone, from the desktop through Microsoft Outlook or a Zimbra e-mail application, or through a Web based e-mail client, or mobile phone application. A Message Waiting Indicator on the phone device can alert you to new messages. Using the configurable Notify Me feature, you can receive notifications of new messages by e-mail, text message, or a telephone call. Messaging also supports e-mail-based pager notifications through SMTP. The current release of Messaging does not support numeric pager notifications. For calls that go unanswered, you can use the Reach Me feature to forward calls to up to three numbers, rung sequentially, according to a schedule you specify. A basic speech Auto Attendant provides outside callers the option to simply say the name of the person present in the Messaging directory that the callers want to reach.

Several Avaya products enhance the Messaging feature set. With Avaya one-X® Speech, you can gain speech access to your voice messages, calling capabilities, enterprise contact directories, and to your e-mail and calendar. Using Avaya one-X® Communicator, you can reach Avaya Aura® Messaging voice messages on your desktop. Using Avaya one-X® Mobile, you can interact with your voice messages through an application on your mobile phone.

The TUI

Two available versions of the Avaya Aura® Messaging TUI facilitate easy transition from Aria and Audix systems. Using the Aria or Audix interface, you will find a familiar menu structure and all the commonly used functions, plus new features and unified messaging capabilities, to help you stay connected with colleagues and customers irrespective of your location. All familiar components of the play functionality are present in the Messaging TUI, including pause and resume, rewind, skip and replay, and increase or decrease speed of play. You can call or reply to the sender, and forward a message with a comment at the beginning, delete or skip messages, or just scan message headers.

In addition to the familiar create and send functions, the Messaging TUI is engineered such that the Messaging key press functions closely match the old Aria and Audix TUIs. Personal distribution list creation and some user preference functions can now be set using a Web application, while some outdated and little used functionality has been removed.

Message notification

Besides the Message Waiting Indicator (MWI) on your desk phone to indicate that you have unread messages, you can configure the Notify Me feature to alert you to new voice messages by text message, e-mail, or by a desk phone call or a mobile phone call. Messaging also supports e-mail based pager notifications through SMTP. The current release of Messaging does not support numeric pager notifications. Using notification through text message, you can specify that Messaging should only alert you when the caller marks the message High Importance. To receive notifications by a phone call, you can opt to turn notification on or off through the TUI. You can also use the Notify Me feature to e-mail yourself copies of voice messages and to include the recording of the voice message in the e-mail.

If you have access to one or more of the Notify Me features outlined in this section, you can configure your personal information on the Notify Me tab of the User Preferences and begin using this feature once configured.

Speech recognition

With speech-based addressing, instead of entering the mailbox number of a person or spelling the name using the telephone keypad, you can simply say the name. Outside callers, too, can say a name instead of entering an extension. The Basic Speech Auto Attendant recognizes first name-last name combinations (for example, William DuBois). To improve recognition accuracy in cases where the correct pronunciation of a name does not follow the pronunciation rules of the primary language, administrators can enter the name phonetically (for example, doobwah for Dubois).

If the confidence level of the speech recognition result is below a certain threshold, the Basic Speech Auto Attendant prompts the caller to confirm the name. The confirmation dialog then uses text-to-speech (TTS) to say the name and prompts the caller again to confirm the name. The caller is given several opportunities to confirm the name, enter an extension number, or the spelling of the name.

Greetings

You can record a single greeting for all circumstances or one greeting for when your line is busy and another greeting for when you are unable to pick up the call. Or you can just use the default Messaging system greeting.

You can also record an Extended Absence Greeting (EAG) message to let callers know that you will be away from the office and won't be able to reply quickly to their messages. Because Messaging only applies EAG functionality when it answers a call, the administrator can block it from recording a new message. However, this ability to block new messages is only available when the call comes through the Auto Attendant or when a user's station sends a call to cover. Messaging will not block messages from users who compose and send a message from within their own mailbox or from their networked contacts.

Attendant and Personal Attendant

You can also use the Attendant feature to field incoming calls. Also called the zero out option, the Messaging system forwards a caller to a live operator if the caller press zero while your greeting is playing. Or you can configure a Personal Attendant to forward your calls to another extension or to any phone number. If no one answers these numbers, the call is forwarded to a live operator at the main extension or to a general delivery mailbox.

Transfer to Messaging

Messaging interoperates with the Transfer to Messaging feature of Communication Manager. The feature is also called Transfer to AUDIX.

With the Transfer to Messaging feature, the operator or attendant can transfer the caller directly to the mailbox associated with the originally dialed number. The transferring party does not need to re-enter the originally called number, and the telephone of the originally called number does not ring again. For other PBXs, Messaging uses a caller application to transfer a caller directly to a mailbox.

Record on Messaging

Messaging interoperates with the Record on Messaging feature of Communication Manager.

With the Record on Messaging feature, you can record a telephone conversation after you answer the call and then store the recorded conversation as a message in your voice mailbox.

When you record the conversation, all participants on the call hear a periodic alerting zip tone. This alerting tone reminds all participants that Messaging is recording the conversation. You can choose the time interval to play the periodic alerting tone. If you set the time interval of the

periodic alerting tone to zero, the participants do not hear the alerting tone. You can also set the alerting tone to play to any one of the following:

- All the participants on the call
- The initiator only who activates the recording
- None of the participants on the call

With the Record on Messaging feature, you can record only one call at a time. Also, attendants cannot use the Record on Messaging feature.

Note:

Some countries, states, and localities have laws that determine if and under what circumstances you can record telephone conversations. Before you administer the Record on Messaging feature, you must understand and comply with these laws.

Reach Me

To further extend your accessibility to callers, you can use the Reach Me feature to control how unanswered calls are handled based on several criteria. You can manage how your incoming calls are forwarded using the following Reach Me configuration options:

- Give priority to the callers in the internal directory.
- Screen the call before deciding to answer by asking the callers to record their name.
- Specify up to three Reach Me numbers to forward calls.
- Set up a schedule to forward calls during certain hours and on certain days.

If you have access to the Reach Me feature outlined in this section, you can configure your personal information on the Reach Me tab of the User Preferences and begin using this feature once configured.

Fax handling

The administrator can configure Messaging to detect and transfer faxes to a third party fax server or to receive and forward faxes to an e-mail inbox you specify. Faxes are stored in the user e-mail inbox and not on the voice mail server and are therefore, not accessible through the TUI. Callers can send faxes directly to a DID or extension.

User Preferences

Although you can set the password and record your name and personal greetings from the TUI, you configure all general preferences and feature settings using a Web-based interface. You can launch the User Preferences Web page directly from the Messaging toolbar within the Outlook desktop client or Zimbra Web Client applications or by typing an easy-to-remember Web address.

General preferences

On the General Web page of User Preferences, you can view your Messaging access numbers and account information and set the time zone for the date and time announcement that plays when you listen to your messages. The time zone setting affects your Reach Me schedule as well as the Notify Me feature. On the General Web page, you can also set the language to be used in the voice messaging system, set the e-mail address for faxes, and specify the telephone number to be used for the Play on Phone option on the Messaging toolbar when accessing voice messages from an e-mail client. On this page, you can also set the number where calls should be forwarded when a caller presses zero while listening to your greeting.

Features settings

On the Reach Me Web page of User Preferences, you must specify how you want your incoming calls forwarded based on whether you use caller priority and call screening. Use this page to set forwarding numbers, the sequence in which the numbers should be called, and the schedule when you want the calls forwarded. On the Notify Me Web page, you can indicate how you want to be notified of pending calls, and enter the appropriate phone number or e-mail address. You can customize the behavior of the TUI on the My Phone Web page and set features such as message playback order, speed of message playback, and whether to use voice recognition when addressing calls. On the Personal Lists page, you can conveniently create and manage multiple personal distribution lists.

For more information, see *Using Avaya Aura® Messaging*.

Personal Lists

A personal list is a labeled collection of addresses that you can create and save for later use. Messaging sends the messages that are addressed to the list to all of the addresses, that is list members, within the list. Users who frequently send messages to the same group of people can create the personal lists for the groups.

You can create the personal lists using the User Preferences Web pages. You can create a maximum of 99 personal lists. Unlike an ELA, the personal lists are created and managed by a user rather than a system administrator. Unlike an ELA, the personal lists are personal, meaning that only the owner of the list can view and use the list.

For more information, see *Using Avaya Aura® Messaging*.

Avaya Aura® Messaging as part of a Unified Messaging solution

The Avaya Aura® Messaging flexible storage capability offers two ways in which you can gain access to your voice mail.

- Dual store: Avaya message store is your storage destination for voice mail, and you use a different storage destination such as Microsoft Exchange or VMware Zimbra for e-mail.
- Single store: You use the same external system for voice mail and e-mail such as Microsoft Exchange or VMware Zimbra.

These scenarios are not mutually exclusive. Administrators can configure Messaging to allow groups or individuals to use their preferred storage solution. When set up on the system, storage destinations are configurable on a per user basis.

If you use the Avaya message store as your storage destination for voice mail, you can unify your voice and e-mail messages at the client level by setting up a separate IMAP4 Messages mailbox in Microsoft Outlook. Your voice mail then appears in a separate mailbox within Outlook. With this solution, you have the option to use Avaya one-X® Mobile to view voice mail in an e-mail format on your mobile phone and gain access to your voice mail on a laptop from any location with Avaya one-X® Communicator.

If you use Microsoft Exchange as the storage destination for both voice and e-mail messages, your voice mail appears in your Outlook inbox automatically. This is message unification at the server level. With this option, you can view your voice mail from any dedicated application on a smartphone, or from any location with Microsoft Outlook Web Access. With Zimbra, Messaging is also unified at the server level, with voice mail accessibility in an IMAP4 e-mail client, through the Zimbra Web application, and through dedicated mobile phone applications.

Personal computer e-mail access

The kind of access you have to Messaging on the personal computer depends on the voice mail storage option you choose. If you store your voice mail in the Avaya message store and set up a separate Avaya Aura® Messaging IMAP4 Inbox in Microsoft Outlook, a dedicated Messaging toolbar appears in the body of the voice mail message when you open the message. From the toolbar, you can play the message on the personal computer or on a phone, reply to a message, forward the message with an introduction, or call the sender. You can also set user preferences and access online help from the toolbar. If you set your user preferences to receive a Notify Me e-mail copy of voice messages, the copy appears in your main Outlook inbox. These copies do not display on the Messaging toolbar. For more information, see

Outlook toolbar GUI Online Help and *Using Avaya Aura® Messaging*, available in the Avaya Aura® Messaging Documentation Library.

If you choose Microsoft Exchange as your destination storage server for both voice and e-mail, you do not have to set up a separate mailbox. Your voice mail appears in your Microsoft Outlook inbox automatically, interleaved with your e-mail messages. As with the client unified option, in which you store your voice mail in the Avaya message store, the dedicated Messaging toolbar appears in the body of the voice mail message when you open the message, and you have the same toolbar functionality.

If you choose the Zimbra Collaboration Server (ZCS) as your storage destination, you have access to your voice mail in the Zimbra Desktop e-mail application. From a toolbar similar to the Messaging toolbar in Outlook, you can play your voice messages on a phone, send a voice reply or voice forward, or call the sender. You can also set user preferences from the toolbar.

Web access

If you choose Microsoft Exchange as your storage destination for voice mail, you can gain access to your Messaging voice mail through a Web browser with the Microsoft Office Outlook Web Access (OWA) application. Using OWA, you can gain access to your Microsoft Exchange Server mailbox from any computer with an Internet connection.

If you use the VMware Zimbra Collaborative Server as your message store, you have similar access to Messaging through Zimbra Web interfaces.

Smartphone access

With the Avaya message store as your storage destination, you can manage your voice message on a smartphone using Avaya one-X® Mobile. For more information, see Avaya one-X Mobile on page 31.

With the Microsoft Exchange server as your storage destination for voice mail, you can access Messaging through the dedicated application on most mobile devices, and view your voice mail in an e-mail style format.

With Zimbra as your storage destination for voice mail, you can obtain access to your Messaging voice mail in a Web interface designed for easy viewing on a mobile device. You can access your e-mail, calendar, and address book.

Avaya one-X® Speech

Using Avaya one-X® Speech, from any phone, you can play voice mails, send, forward, reply, and delete messages, and save messages to a predefined folder. You also have the ability to

screen incoming calls through the Reach Me feature and set reminders and schedule appointments.

With the Avaya message store as your storage destination, you can use Avaya one-X® Speech to retrieve your Messaging voice mail. With the Microsoft Exchange server as your storage destination for voice mail, you can retrieve your voice mail in an e-mail style format. Avaya one-X® Speech does not provide access to voice messages if you use Zimbra.

For more information, see the Avaya one-X® Speech client product documentation (Site Preparation Guide, Installation Guide, and Wallet Card) available at https://support.avaya.com/css/Products/P0519/All_Documents.

Avaya one-X® Communicator

Avaya one-X® Communicator provides desktop access to your voice messages from a single, intuitive user interface.

Avaya one-X® Communicator does not work with Exchange or Zimbra. When you choose the Avaya message store as your destination storage server for voice mail, you can gain access to Messaging through Avaya one-X® Communicator and listen to and respond to voice mail, make calls, and view fax messages on your personal computer. With Avaya one-X® Communicator you can gain access to all the features you have on your phone, plus voice-video calling, visual voice mail, and voice-video conferencing capability, using which you to join several calls together in a ad hoc conference. You can gain access to your personal contacts list and to the complete corporate directory, and can view your communications log, where calls you receive even when you are not logged into Avaya one-X® Communicator, are tracked.

You can use Avaya one-X® Communicator to perform the following actions:

- Listen to a voice message
- Delete a voice message
- Call the sender of a voice message
- Add a number from a voice message to personal contact
- Add a number from a voice message to Favorites
- Mark a voice message as read or unread

For more information, see the Avaya one-X® Communicator documentation at https://support.avaya.com/css/Products/P0516/All_Documents.

Avaya one-X® Mobile

Avaya one-X® Mobile provides a graphical interface to gain access to the Messaging voice messages. You can use Avaya one-X® Mobile to both see and hear voice messages on your mobile phone. You do not need to dial into the system because messages are automatically downloaded to the handset in the form of sound files. As all messages are visible in a list with the sender name and duration, you do not have to sort for important messages.

For more information about Avaya one-X® Mobile, see the Avaya one-X® Mobile documentation at https://support.avaya.com/css/Products/P0438/All_Documents.

Chapter 3: Administration features

Class of Service

A Class of Service (CoS) defines the privileges and the features assigned to a group of users. You can use the Class of Service page to define each CoS, create new CoSs, and change or rename existing CoSs. You can use the User Management page to assign a previously defined CoS to a user. The Basic and Mainstream licenses control the features. The CoS definitions determine which features are available for users assigned that CoS. The CoS definition determines whether a basic or mainstream license is required for users that use that CoS. The maximum storage size for a CoS is 65536 KB.

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

- Standard: Use to allow local and domestic long-distance dialing.
- Enhanced: Use to allow local and domestic long-distance dialing.
- Executive: Use to allow local, domestic long-distance, and international dialing.
- Info Mailbox: Use to create a message for an info mailbox. A typical informational message might include details about directions, business hours, weather, or human resources. You can record messages for an info mailbox that take up to five minutes to play. You cannot create an info mailbox by assigning the Info Mailbox CoS to the user.
- Administrator: Use 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 also determines which users can send broadcast messages. This CoS is unrelated to the administrative privileges handled through the Server (Maintenance) RBAC administration.
- ELA: Use to use the Enhanced-List Application.

For more information, see *Administering Avaya Aura® Messaging*.

System Management Interface

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

SMI has three interfaces:

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

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

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

Certificate Signing Request

Using Messaging, you can install your vendor signed certificates on your Messaging systems. Using your vendor signed certificates help to alleviate the errors you receive while logging into the SMI. A trusted certificate must be a Certificate Authority (CA) certificate and built for a particular system name, that is, fully qualified domain name.

You can use the Certificate Signing Request (CSR) Web page to manage the CSRs present on the server. You can generate a CSR to send to your CA, that is, Entrust and VeriSign. For more information, see *Administering Avaya Aura® Messaging*.

Role-Based Access Control

With Role-Based Access Control (RBAC), you can control privileges on the application server and storage server based on the roles defined for the business. Using roles, you can fine-tune the security and administration of the Messaging system. A role defines a group of users who have certain privileges. You can create roles to allow or restrict access to the SMI Web pages as desired.

You can group the access rights by a role name. Profiles for access to SMI Web pages are named *access masks*. Using the access mask, you can restrict the access permissions. Messaging provides some default access masks and names, such as System Profile, Customer Super User Profile, and Customer Non-Super User Profile. You can use SMI to create a new Web access mask profile and enable access as desired.

For more information, see *Administering Avaya Aura® Messaging*.

Caller Applications

Caller Applications are a collection of menus and prompts by which administrators can extend the Messaging caller interface. Using Caller Applications, administrators can extend the Automated Attendant depending on the requirements of the organization.

The basic functions that a Caller Application provides include:

- Defining a full call menu structure with up to nine options for users to select. For example, transferring callers to a specified mailbox.

  A mailbox can have one primary extension number and one or more secondary extension numbers. Callers are transferred to the requested mailbox extension.
- Defining business hour and off-hour schedules for the organization, as applicable.
- Defining holiday schedules for the organization, as applicable.
- Configuring prompts by uploading voice-based prompts if required by the caller menus, or entering Text-to-Speech prompts.
- Defining call menus in support of business hours, off-hours, and holiday schedules.

The Caller Applications Editor creates Caller Applications.

Caller Applications Editor

Caller Applications Editor is a software application that consists of Microsoft Management Console (MMC) snap-ins and extensions. The Caller Applications Editor creates Caller Applications. Upon creation, Caller Applications are automatically deployed to the storage server and to the relevant application servers.

Caller Applications Editor can run only on a Microsoft platform that can communicate with the storage role server to deploy the created Caller Applications.

System broadcast message

The administrator defines using the Administrator CoS which users can send broadcast messages. If the administrator has activated the system broadcast message feature using the Administrator CoS for you, you can use the system broadcast message feature to send a message or an announcement to all local users. The system broadcast message is available to the user only on the TUI and not while using IMAP4 within Microsoft Outlook. Hence,

Messaging does not send any notification to the user for the system broadcast message. Broadcast messages do not light the MWI on the user's desk phone.

You can only have one broadcast message at a time. If you want to send another broadcast message, the second message overwrites the first broadcast message. Recipients of a broadcast message can only access the most recent broadcast message at any given time. If a user does not log in and access a broadcast message, and you send another broadcast message, the users do not hear the first broadcast message.

As the system broadcast messages typically provide information related to system administration for a cluster of application servers, the system broadcast message is available even when Messaging is operating during an offline mode.

The administrator typically activates the system broadcast message feature to a limited number of users within the organization.

Messaging also provides the following full-featured distribution lists:

- Enhanced List Application. See Enhanced List Application on page 36.
- Personal Lists. See Personal Lists on page 27.
- Message Networking Enterprise Lists. See Enterprise Lists on page 36.

Enhanced List Application

Using the ELA CoS, the administrator defines which users can use the Enhanced List Application (ELA) feature. Users can use the ELA feature to create distribution lists for delivering messages to a large number of recipients. ELA associates one mailbox to a list of members, so that when users want to send a message to the whole list, the users can send a message to the list mailbox instead. When a new message is delivered into the list mailbox, known as the shadow mailbox, ELA distributes the message to the members of the list. ELA members can be local or remote users.

For more information, see *Administering Avaya Aura® Messaging*.

Enterprise List

You can also use Message Networking Enterprise Lists, which are enterprise-wide mailing lists for users that reside on a Message Networking system. Each Enterprise List represents a specific group of potential recipients for enterprise distribution messages. For more information, see *Message Networking Concepts and Features Guide*, available at the Avaya support Web site at http://support.avaya.com.

Backup capabilities

The Messaging server backs up Messaging data over the customer 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. Messaging data backup may easily reach 50 Gigabytes or more. Customers may be unable to support transfers of single files of this size. Hence, Messaging data backup consists of multiple files, small enough to be transferred in a customer environment.

Messaging supports the File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), and Session Control Protocol (SCP) backup methods. The system administrator who is administering network backups needs to be aware of the possible file storage sizes and the limitations of the storage size on the customer data network.

A system administrator can limit the user mailbox size of storage so that users do not have more than 10 minutes of voice storage in the mailbox. A system administrator can also limit the number of days a message can remain in a mailbox before the message is deleted. Currently, the system default is 45 days, that is, a message remains in the mailbox for 45 days before being deleted. The system automatically deletes messages during the nightly audits after the message age equals the administered number of days.

Chapter 4: Messaging solution architecture

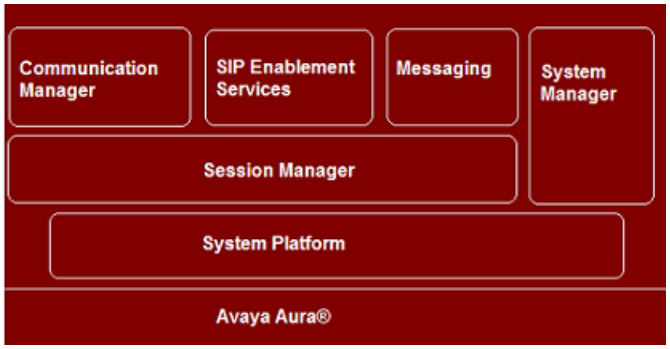
Avaya Aura®, the latest core communications architecture from Avaya, represents a new approach to business communications that simplifies complex multivendor, multimodal, multilocation networks to create a truly unified architecture.

By simplifying complex communications networks, Avaya Aura® reduces infrastructure costs and delivers voice, presence, messaging, video and Web applications to users, irrespective of the location of the employees. Avaya Aura® adds powerful new capabilities to Communication Manager, including session management that enables multivendor hardware and software to communicate across the enterprise. Avaya Aura® unifies a wide array of communications applications and systems, decoupling them from the network so that services can be deployed to users depending on what users need rather than by where the users work or the capabilities of the system to which the users are connected.

Avaya Aura® supports single cross-enterprise dial plans and centralized administration, reducing operating costs and speeding up rollouts of new applications. New aggregated presence features and the inclusion of Avaya one-X® Unified Communications interfaces allow businesses to take full advantage of unified communications applications and solutions.

For additional documentation, see the Avaya support Web site at http://support.avaya.com.

Avaya Aura® components



The following components provide the Avaya Aura® core communications services:

- Avaya Aura® Communication Manager. The open, highly-reliable and extensible IP telephony foundation on which Avaya delivers intelligent communications to large and small enterprises.
- Avaya Aura® SIP Enablement Services. Delivers rich communications, collaboration, mobility, and application integration capabilities to the enterprise.

- Avaya Aura® Messaging. A part of the Avaya Aura® architecture, but Messaging can also be used in other environments. For more information, see Avaya Aura Messaging overview on page 9.
- Avaya Aura® Session Manager. A SIP routing and integration tool and the core component of the Avaya Aura® solution. Session Manager integrates the SIP entities across the entire enterprise network within a company. Session Manager offers a new perspective on enterprise communication where individual locations are no longer managed as separate units within the enterprise. Each location, branch, and application is viewed and managed as part of the overall enterprise.
- Avaya Aura® System Manager. A product that takes a solution-level approach to network administration. IT departments can use System Manager to incorporate new components and applications under a common management umbrella over time, managing all the elements of Avaya Aura® together as a system. System Manager centralizes provisioning, maintenance, and troubleshooting to simplify and reduce management complexity and solution servicing. System Manager provides a common management framework that reduces the complexity of operations for distributed multisite networks with multiple control points inherent in SIP. System Manager also increases the value of convergence through tight integration with the enterprise IT infrastructure.
- Avaya Aura® System Platform. A product using which you can consolidate applications in a single server, decreasing your hardware footprint, cooling and energy costs. Because of this consolidation, you may need fewer servers for the same configuration than with other competing products. For more information, see System Platform on page 40.

For additional documentation, see the Avaya support Web site at http://support.avaya.com.

System Platform

System Platform is a generic virtual server software platform that provides a common set of features and services. This set of features and services allows preinstalled and configured virtual applications, called solution templates, to reside on a single physical server.

System Platform is Xen-based and includes the following:

- Base CentOS Linux system running the Xen Hypervisor (Dom0)
- Web-based management console for installing and managing templates
- Virtual machine for System Platform system utilities

System Platform features include:

- Secure Access Link (SAL) to handle alarming and remote access
- A consistent upgrade method for all patches and products in the solution template
- Security that conforms to Avaya product security standards
- A Web License Manager (WebLM) server to manage product licenses
- A Network Time Protocol (NTP) clock synchronized to a customer-provided NTP server

Virtual Machines

System Platform includes CentOS as the base operating system, the Xen Hypervisor, and a virtual machine (CDOM) that is used to manage the platform. System Platform includes the following:

- System Domain (Dom0): In addition to exporting virtualized instances of CPU, memory, network, and block devices, Xen displays a control interface to manage how these resources are shared between the running domains. Access to the control interface is restricted to a specially privileged virtual machine, known as domain 0 or System Domain.
- Console Domain: Console domain is a virtual machine, which is a part of System Platform, and has many platform elements such as:
  - Common logging and alarming
  - Remote access
  - System Platform Web Console
  - Upgrades and patches
  - WatchDog
  - Licensing
- User applications domain (udom): User applications domain is a virtual machine used to run with a specific type (or mode) of High Availability protection, according to Avaya Aura® solution template requirements.

Template

All Messaging systems are installed on System Platform using a template. Avaya offers product-specific templates to install different products on System Platform. A template is a definition of a set of one or more applications to be installed on System Platform.

Messaging offers the following templates:

- Msg_Standard.ovf. The Messaging template for the standard server.
- Msg_4x146GB_HDD.ovf. The Messaging template for the high capacity storage server.

For more information on templates, see *Implementing Avaya Aura® Messaging*.

Switch integration

Switch integration is the means by which the switch and the Messaging system exchange control information about calls. Switch integration is achieved when a call is presented to a voice port and information about the call is supplied to the Messaging system. This information includes the nature of the call, called party information, and the calling party number.

Messaging supports only Session Initiation Protocol (SIP) integration. SIP is an important technology for establishing real-time audio and multimedia calls in a converged IP network environment.

Using SIP, the switch and the application servers are connected to the local area network (LAN). All exchange of information, such as call information, signaling information, and voice data, happens over voice channels through the LAN.

You can connect the Messaging system to the switch, using the SES proxy or Session Manager, through SIP trunks. The SIP trunks are administered as part of a trunk group on the switch. You can also directly connect the Messaging system to the switch without using the SES proxy or Avaya Session Manager. Consult your ATAC or Sales Engineer representative for these types of integration.

Messaging interoperates with AudioCodes gateway to work with switches and integrations that are not supported. You need one AudioCodes gateway for each application server. If you need more than one gateway to meet the port capacity, you will need extra application servers. Analog gateways, for example, can be limited to 24 ports. Therefore, 96 ports require three gateways and three application servers. For N+1 configurations with a single AudioCodes gateway, you can configure a single AudioCodes gateway to load balance the traffic across multiple application servers.

Hardware

Depending on the mailbox capacity, Messaging offers the following two types of servers:

- Standard Server
- High Storage Capacity Server

For more information, see *Implementing Avaya Aura® Messaging*.

Supported hardware

Messaging supports the following Avaya-provided hardware:

- Dell™ PowerEdge™ R610 Server
- HP ProLiant DL360 G7 Server
- S8800 Server
- S8730 Server

You can use any of the mentioned servers for new installations of the Messaging solution. Messaging systems upgraded to the Messaging Release 6.1 system can use Dell PowerEdge R610 Server, HP ProLiant DL360 G7 Server, and S8800 Server.

If you are an existing customer of Avaya and have S8730 server, you can install Messaging on your existing S8730 server after upgrading the S8730 server with the required memory and hard drive upgrades. For more information on the S8730 server upgrade, see *Maintaining the*

S8730 server for Modular Messaging available at https://support.avaya.com/css/Products/P0792.

Messaging architecture

The Messaging system consists of one or more servers that perform specific roles. At the heart of the system is a server that performs the storage role. This server is supported by multiple servers in an application role, handling the telephony role, as long as the total number of ports within the system does not exceed 300.

System

A system is simply a way to describe the physical collection of servers that act together to provide functionality to a set of users. A system may span multiple locations, have multiple sites, or contain multiple clusters but has only one directory.

Server

Using the flexible architecture of Avaya Aura® Messaging, you can customize your messaging system to fit your business needs. When you first set up your Messaging system, you assign roles to the servers. As your business changes and grows, you can add new servers and reassign the server roles.

Server roles

The Messaging system is designed to perform two distinct functions or roles. These roles are:

- Storage role
- Application role

These roles are independent of the server on which the roles reside. Using the Messaging architecture, you can change the role of the server. For example, you can change a single-server system into a two-server system in which the original server plays the storage role, and the newly acquired server plays the application role.

Storage role:

The storage role stores:

- Voice messages (When using the Avaya message store)
- Directory data in an LDAP directory (users contacts, distribution lists, caller applications)

The storage role also supports nonvoice interaction with users, including:

- IMAP4 access to voice messages (When using the Avaya message store)
- SMTP routing of voice messages, text-message notifications, and e-mail copies
- Connectivity to:
  - The LDAP directory
  - The message store for monitoring Message Waiting Indicator (MWI) and Notify Me (text message notifications, telephone call notification, and e-mail copies)
  - User Preferences

Application role:

The application role supports real-time telephony interaction with users and callers, including:

- Integration with your telephony system for voice and MWI
- A telephone user interface for users and callers, including Auto Attendant and Caller Applications
- Local caching for the offline handling of user directory data, greetings, recorded names, and voice messages

Note:

In the offline mode, IMAP only shows messages that have reached the storage server. Messages that are only in the cache on the application servers are not accessible with IMAP during the offline mode.

Server types

Server types refer to the functionality of the server. All servers share the same software and the same System Management Interface (SMI). The type of an Avaya Aura® Messaging server depends on the role the server assumes. The server types are:

- Single server. A server that combines the application and storage roles.
- Dedicated storage server (also called a storage server). A server that is identical to a single server except that only the storage role has been enabled.
- Dedicated application server (also called an application server). A server that is identical to a single server except that only the application role has been enabled.

A server can support up to 100 ports of active traffic.

Message store

When the Avaya message store is the storage destination for user messages, the message store resides on the same server that performs the storage role. When a third-party server is the storage destination for user messages, the message store resides on a third-party, corporate storage server.

When you use a third-party storage server, your system still requires at least two Avaya servers: one for the AxC/Directory server, and one or more for application servers.

You can use the AxC/Directory server for notification capabilities, the LDAP database, and to provide communications between the application servers and the third-party storage server. You can also use the AxC/Directory server to store user properties, name, and greeting recordings. All voice messages are stored on the user's third-party storage server.

System configuration

You can combine servers of different types to make a system, although only one storage role can exist in a system. This server may be a dedicated storage server or a single server with both the storage and application roles combined with or without additional dedicated application servers. The system therefore is versatile enough to meet different implementation needs of customers from a single box solution for a small office to front-end/back-end topologies, where the front end performs the application role and the back end performs the storage role. You can design your system so that the location of the front-end application servers is remote from the back-end storage server. This flexibility allows you choose either distributed or centralized system topologies for your organization.

When your system requires more than one server, Avaya recommends that one of the servers be a dedicated storage server. Messaging is designed to provide redundancy through a distributed cache mechanism in case the storage server becomes unavailable. However, this redundancy cannot be fully achieved if part of that cache is also on the storage server.

System behavior

Each server that performs an application role is capable of handling calls and ultimately recording a message. Directory information and user greetings are cached within each application role in order to provide a smooth experience to external callers. When a message is left, the message is initially cached within the local application role before being forwarded through a connector (AxC) to the appropriate message store. The AxC, which is provisioned by the storage role, is capable of communicating with each supported message store type.

When a user logs on to Messaging to retrieve messages, a definitive list of messages is fetched from the message store through the AxC. If the audio part of the message is available in the

local cache then this part is used to play back the message, otherwise the audio part is also retrieved from the message store using the AxC.

Sites

Any Messaging system can contain multiple sites. Each user is associated with a site and each site has own properties including:

- Access number
- Extension length
- Mailbox length
- Auto Attendant

Where sites are used, the directory for the site defaults to only users within the site. However, directory entries from other sites can also be included

Each application role can only belong to one site and has its own configuration such as language and time zone, which should be consistent for all servers in the site.

Clustering (Topology)

Clusters can improve the resilience and capacity of the Messaging system by allowing multiple servers that perform the application role to act together. You can combine up to three application servers to form a cluster and add a fourth server for redundancy as long as the active traffic does not exceed 300 ports. You can use a maximum of four application servers per system.

Clustering also replicates user data, such as passwords and greetings, in real time to ensure seamless service between each member in the cluster. However, updates to application roles within other clusters occur only at the time of the nightly maintenance routine.

Clusters are typically designed based on physical location and each application role is configured identically. If you want to retrieve messages when either the storage role or mailbox store is unavailable, a member of a cluster combines a list of available messages from the other servers within the cluster.

Starting with Avaya Aura® Messaging 6.1 and later, members of a cluster regularly test connectivity with other members of the same cluster so that if one member becomes unavailable, prolonged delays are not encountered when trying to obtain a message from another server.

You can have multiple clusters within a system as long as the system maximum port capacity of 300 is maintained.

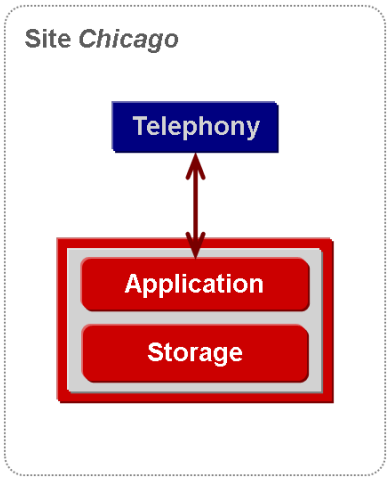
Server configuration

Single server

In a single-server topology, the application role, AxC/Directory role, and optional storage role are active on the same server. The application role integrates with the telephony server.

Note:

You cannot use a single-server configuration with a third-party storage server. For more information on server requirements, see Message store on page 45.



Front-end/back-end

In front-end/back-end topologies, the front end plays the application role and the back end plays the storage role. Dedicated application servers communicate with the telephony server and the AxC that resides on the Avaya message store.

You can design your system such that the location of the front-end application servers is remote from the back-end storage server. This flexibility allows you choose either distributed or centralized system topologies for your organization.

Clustering

You can combine up to three application servers to form a cluster and add a fourth server for redundancy as long as the active traffic does not exceed 300 ports. Each cluster supports flexible, per user message stores. The message store can be the Avaya storage server, a Microsoft Exchange server, or a VMware Zimbra server.

Using clustering application servers, you can increase the system capacity to support more users. Every application server increases the number of available ports.

Clustering also provides redundancy for all application servers in a cluster because all application servers within a cluster are configured identically and are therefore interchangeable.

Clustering handles data as follows:

- User passwords and greetings are replicated on each clustered application server.
- Messages are distributed among the clustered servers.
- The global address list (GAL) and personal user lists are synchronized on each application server during the nightly maintenance.

Mixed storage configuration

With the flexible architecture of Messaging, you can mix different types of storage servers on the same system. Using this flexible design, you can continue using e-mail servers in your network environment.

Using a mix of different storage servers on the same system, you can also choose the location where Messaging sends the voice messages of an individual user. This flexibility helps you to address discovery and compliance concerns. This flexibility also ensures that you are not locked into the product of a specific e-mail vendor.

The Avaya storage server:

- Uses LDAP to provide directory services
- Relays messages between the application server and third-party servers
- Stores voice messages

You can turn off the storage functionality, if needed. However, Messaging requires the Avaya storage server to provide other services.

Mixed storage examples

The Messaging administrator determines the storage destination for the voice messages of each user. Because the storage destination is determined on a per user basis, users can use their current e-mail server for storing voice mail.

- In a single storage configuration, the administrator turns off the message storage function of the Avaya storage server, and all messages are relayed to the third party server.
- In a dual storage configuration, the administrator configures the system so that some messages are stored on the Avaya storage server and others are stored on the third-party server.
- In a triple storage configuration, the administrator can distribute messages between the Avaya storage server and two third-party servers.

Network topology design

Your messaging network topology is determined by the way your organization has identified its sites.

Typical network topologies include sites with:

- Distributed application roles
- Centralized application roles

Small organizations typically require an easy-to-deploy single-server topology that is ready to grow with the needs of the organization. Large organizations can use the examples discussed in Planning for Messaging on page 57 as building blocks for their enterprise-wide network architecture, including:

- Conforming to an existing network topology
- Fitting into centralized data centers
- Supporting local survivability networks
- Meeting high availability requirements
- Supporting disaster recovery requirements

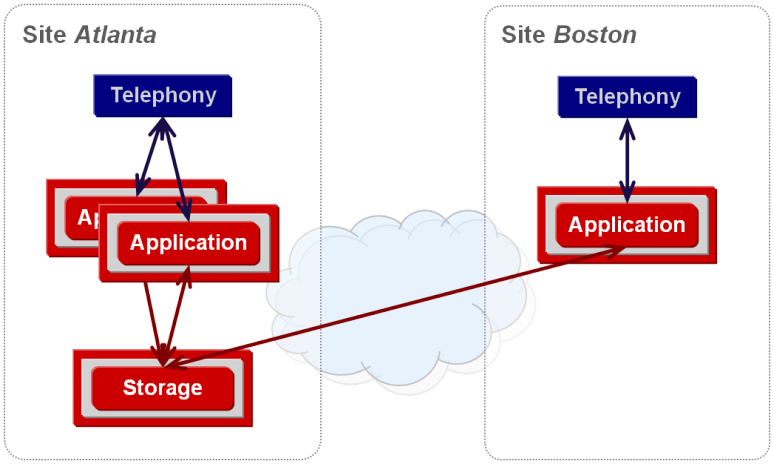
Note:
An application server can support only one site.

Distributed topology

A distributed topology exists when application servers are located within the supported sites.

This topology typically consists of one location that includes a dedicated application server and a dedicated storage server. Remote locations have a dedicated application server but no storage server.

The following image is an example of a topology with two sites, Atlanta and Boston. You can also create a distributed topology of more than two sites.



In this example, there are three application servers: two in Atlanta and one in Boston. Each application server communicates with its local telephony server. However, all the application servers communicate with the dedicated storage server that is located in Atlanta.

Benefits of a distributed implementation

If you want to keep voice traffic to a minimum on WAN and if uninterrupted Messaging service to remote locations, that is, local survivability, is important to you, the distributed model might be more appropriate for your organization. The distributed implementation model itself is a form of redundancy. To ensure continued service, you can add an extra application server for redundancy at locations where local survivability is critical.

With the distributed model, if an application server at a remote location cannot reach the central storage server, the caller experience at that location is the same as if the storage server was reachable. Call answering continues to function and users can still access their most recent messages. For more information about how Messaging continues to function when the storage server is unreachable, see Local survivability on page 53.

The principal benefits of a distributed topology are local survivability and less voice traffic on the network. The tradeoff is a slightly higher total cost of ownership.

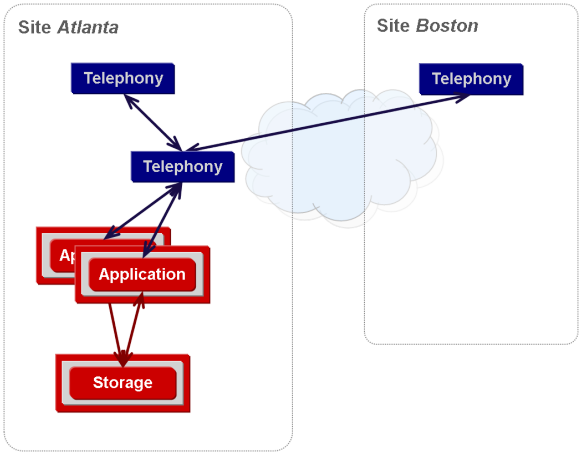
Centralized topology

A centralized topology includes the following network topologies:

- All Messaging servers are at the same location.
- Messaging supports several locations but all application servers are at one location.
- Messaging supports several locations and the application servers are divided among a small number of locations.

This topology accommodates telephony servers with either uniform or mixed dialing plans.

The following image is an example of a centralized topology in which all Messaging servers are at the same location and the system supports users at a different location.



In this example, the second telephony server in Atlanta uses SIP trunks to connect the Messaging system to the telephony servers in Atlanta and Boston. You can administer SIP trunks as part of a trunk group on the telephony server.

The following products typically provide SIP connectivity. See your account representative for a complete list.

- Avaya Aura® SIP Enablement Services proxy
- Avaya Aura® Session Manager
- AudioCodes gateway. You need one AudioCodes gateway for each application server.

Centralized implementation

When you use the centralized topology, you simplify your IT management and lower your total cost of ownership compared to a distributed topology. However, when remote locations connect to Messaging servers over a WAN, your network carries a significant amount of voice traffic. In case of an outage in the network, users at the remote location have no access to the Messaging system until the network is restored. But if you have a high-quality network, your

remote locations are not prone to network outages, or your WAN link is inexpensive, the centralized model might be the solution for your organization.

Benefits of the system architecture

The Avaya Aura® Messaging system architecture is designed to accommodate everything from the relatively small, single location organization, to the large, geographically distributed enterprise with multiple, networked messaging installations. The key benefits of the architecture include the following:

- Flexibility
- Redundancy
- Local survivability

Flexibility

A benefit of the system architecture at the user level is flexible storage capability. You can use the Avaya message store, or Microsoft Exchange, or VMware Zimbra Collaboration Server (ZCS) as your storage destination for voice mail. Or, you can implement a mixture of storage destinations and set up groups or individuals within your organization so that users can select the storage destination.

At the next level, the architecture gives you the option to install a single server or to choose the front end/back end model. You can also convert later from a single server to the front end/back end model by dedicating the machine as your storage server and adding an application server or a cluster of application servers to scale with your increasing voice traffic needs. To protect against loss of messaging service or data, you can add an additional application server to the cluster for redundancy.

At the highest level, the system architecture gives you the flexibility to centralize your application and storage servers at one location or distribute your implementation by placing application servers at branch locations. The system architecture gives you the flexibility to centralize most of your implementation while distributing some sites, where local survivability is critical.

There is no one right solution for all organizations. The flexibility of the architecture gives you a range of deployment options to fit your needs. The scalability of the architecture offers you the advantage to increase capacity by adding servers as your organization grows without changing your topology. The interoperability of the architecture ensures that you can integrate Messaging into your existing network.

Redundancy

When one application server is sufficient to handle all the voice traffic for a location, adding another application server into a cluster provides redundancy. While both servers are online, the servers share the traffic load. But if one server fails, the other server must handle all the traffic. As long as voice traffic is within the capacity of one server, you have full redundancy and there is no interruption of service and no loss of data.

If the traffic requirements require a cluster of two application servers running at or near capacity and you add a third server, the traffic is spread equally among the three servers. If one of the servers fails, the traffic load is divided between the two remaining servers. As long as the traffic is within the carrying capacity of the remaining two servers, there is no interruption of messaging service and no loss of data. The behavior is the same in a cluster of four servers.

Local survivability

Local survivability refers to the continuation of Messaging service in case an application server is unable to reach the storage server. Therefore, local survivability only applies to locations in which an application server is physically present. Local survivability does not apply to single server configurations.

The AxC/Directory server provides connectivity between the application server and a third-party message store. In these configurations, local survivability applies in case any combination of the following connections fail:

- The connection between the application server and the AxC/Directory server
- The connection between the AxC/Directory server and the third-party message store

When an application server is unable to reach the storage server, the application server operates in the offline mode. The offline handling of messages and user directory transactions is the mechanism that Messaging uses to achieve local survivability. Because offline handling is session based and because an application server only uses offline handling when the application server cannot reach the storage server, individual users who do not have an account on the affected application server experience no change in service.

In a distributed topology, all locations have a local application server and therefore, local survivability applies. All application servers use a WAN to connect to the storage server or to the third-party message store through the AxC/Directory server, regardless of their location. For more information, see Distributed topology on page 49. If an application server loses this connection, the application server operates in the offline mode and Messaging continues to function.

In a centralized topology with multiple locations, users at locations that do not have an application server do not have local survivability. These users are connected to Messaging by the network connection between two telephony servers. For more information, see Centralized topology on page 51. If there is an outage in this network connection, users at the location that

has no application server lose Messaging service. However, if the outage is in the connection between an application server and the storage server, the affected application server operates in the offline mode and service continues for all users.

When an application server operates in offline mode, Messaging continues to operate almost as the application server does when the application server can interact with the storage server. For more information, see Limitations of local survivability on page 55.

Cache for messages

Local survivability is possible because each application server has a built in Avaya Distributed Cache (ADCS). This rolling cache holds messages for three days, that is, 72 hours, but you can change this duration to suit your business requirements.

The system caches messages on the application server and then immediately attempts to deliver the message to the storage destination of the recipient when:

- A caller leaves a message (Call Answering).
- A user plays a message (Message review using a TUI).
- A user sends a message (Voice messaging).

After 72 hours, the message is deleted from the cache on the application server. So if the user plays a message that is older than 72 hours, the system retrieves the message from the message store. Then the system caches the message again on the application server as if the message was a new message.

Callers can use their TUI to address a message to multiple recipients by:

- Creating an ad hoc list
- Selecting a predefined personal or system distribution list from their address directory

When the caller sends a message to an ad hoc list, the application server only caches the message in the mailbox of the first person on the list. But after the message reaches the storage server, the system delivers the message to all the recipients. After a recipient who is not first on the ad hoc list plays the message, the system caches the message on the application server for that user.

When a recipient retrieves a message, the application server goes to the storage destination of the recipient to get a list of the recipient messages and their state, that is, unread, read, or saved. For the content of the message, the application server first looks locally in its own cache. If the message is not present in the local cache, the application server looks in the other application servers in the cluster. If the message is not on any of the application servers, the application server retrieves the message from the storage destination of the recipient and places the message into the local cache of the application servers.

Limitations of local survivability

When an application server is in the offline mode, users with an account on that server do not have access to the services provided by the storage server, including:

- Access to clients that depends on IMAP4, for example, Avaya one-X® products and e-mail clients.
- The ability to change User Preferences.
- Message notification features.
- Access to messages that are not stored in the cache of the affected application server.

Avaya recommends that you consider this information when you design your system for redundancy and survivability.

Message notification

If the storage server is not accessible, the Notify Me feature and the Message Waiting Indicator on your desk phone become inoperative, so you must periodically check for new messages. When you log in to retrieve messages, you hear a system prompt that explains that normal access to your mailbox is unavailable.

Message review

You can play any message that is in the cache, including messages that you deleted in the 72 hours before the event that made the storage server unreachable. You can also play any new message from external callers that arrive after the event that made the storage server unreachable. However, while your application server is operating in the offline mode, the system cannot display the message status, that is, unread, read, or saved.

Messages addressed to multiple recipients:

The method the sender uses to address a message to multiple recipients affects how the application server caches the message and therefore, whether you can review the message.

- If you are the first recipient on an ad hoc list, you can play the message as discussed.
- If you are not the first recipient on the list, you will not receive the message until the storage server becomes available.
- Your position on personal or system distribution lists is irrelevant. You will not receive these messages until the storage server becomes available. And you cannot play messages that arrived in your mailbox before the event that made the storage server unreachable unless you played the message before the event and caused the application server to cache the message.

Messages from internal callers:

You can review new, incoming messages when your application server is in the offline mode if you and the sender have an account on the same application server. You can also review the messages if the sender has an account on a different application server if:

- The two application servers are in the same cluster.
- The status of both servers is Active in the **Sites / Application Servers** table on the Topology SMI page.

Chapter 5: Planning for Messaging

Planning for your Avaya Aura® Messaging installation involves a simple equation. On one side, you have the Messaging system with its various components and the capabilities and capacities of the components. On the other side, you have your organization, which includes your network and a certain number of people, in one or more locations, carrying out work that varies from routine to time-critical. The goal of planning is to assess all the factors and variables on both sides of this equation and make the factors and variables equal. In planning your Messaging implementation, you essentially pair up your resources and needs with the capabilities and features of the Messaging system.

Single server configuration

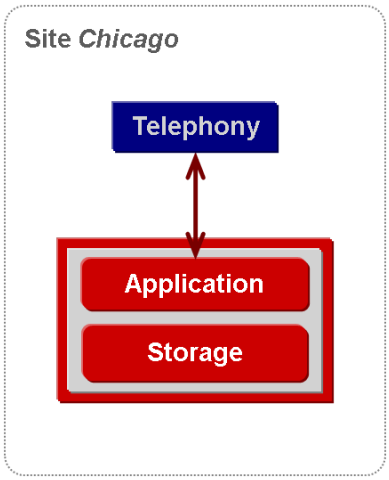
The simplest Messaging implementation is the single server, single site configuration, in which the application role and the storage role are performed by a single virtual machine within System Platform. The single server configuration is an ideal solution for organizations up to a maximum of 5,500 users.

A benefit of this configuration is that if you have fewer than the maximum number of users at your main site, you can add additional application servers at remote office locations. With this scalability, you can easily expand your single server configuration to other Messaging configurations. For example, you might have 2,000 users at your main site and several remote locations with a few hundred users each. In this case, you can add remote users either by placing application servers at those locations or by servicing those users at other sites over WAN, up to the maximum 5,500 users. For this reason, the single server configuration works well for small or distributed organizations and can accommodate such organizations as the organizations grow.

A restriction applies, however. You can add application servers to a single server configuration. But you cannot configure application servers into a cluster with the application role that is on the single server. To expand your single server system into a system with clustered application servers, you must first put the application and storage roles on to dedicated servers. Then you can add other application servers as needed. You cannot use a single-server configuration with a third-party storage server. For more information on server requirements, see Message store on page 45.

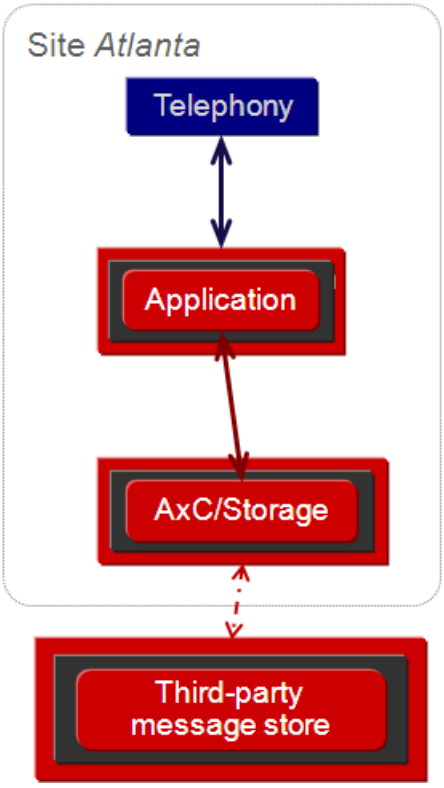
Note:

An application server can support only one site.



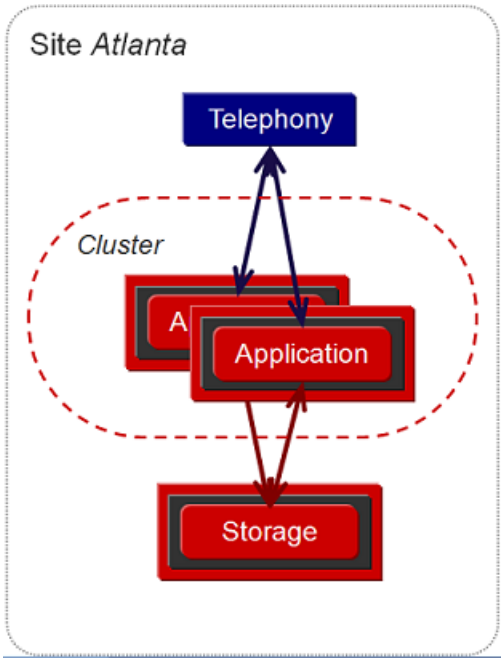
Front-end/Back-end single site configuration

Although the basic front-end/back-end single site configuration, which supports 6,200 users, offers only slight more capacity than the single server configuration, the advantage the front-end/back-end single site configuration offers is scalability. If you expect your organization to grow, you can easily increase capacity by installing a second and a third application server, plus an additional server for redundancy. For more information, see Capacity planning for an Avaya message store on page 64.



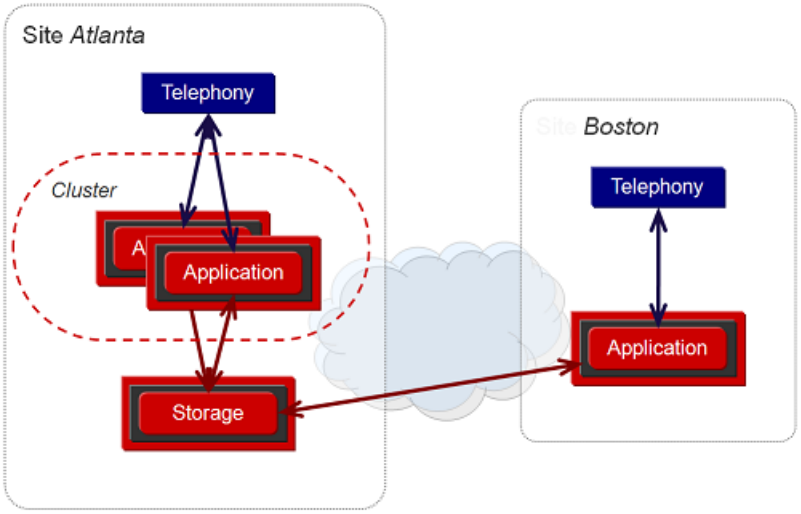
Front-end/Back-end cluster single site configuration

Scalability and redundancy are the two reasons to choose a cluster configuration. You can group up to three application servers in a cluster, plus a fourth application server for redundancy. With 100 ports per server at 62 users per port, three servers support 18,600 users. The maximum number of active ports per cluster is 300.



Distributed multiple site configuration

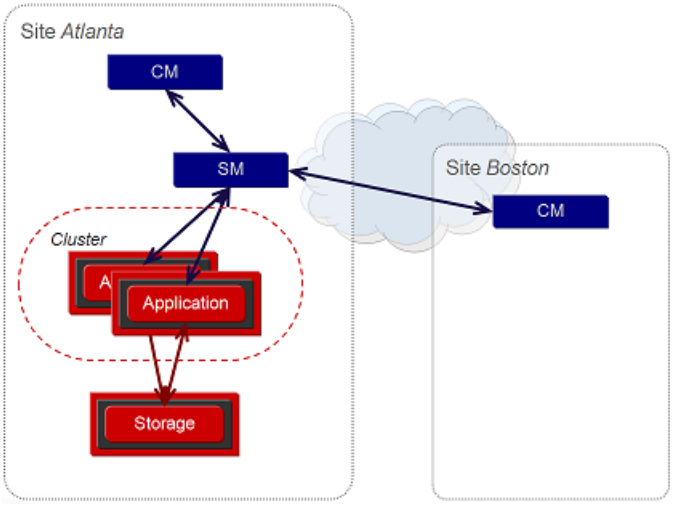
The principle reason to distribute your implementation is local survivability. You can distribute your entire network and place application servers at all location or just those segments where messaging service should not be interrupted. By placing applications servers at remote sites, you can ensure continuation of messaging service in the event of a network outage between the remote site and the main location. If the storage server at the main site becomes unreachable to the local server, users at the remote site experience virtually no difference in service and can retain user messages of the previous 72 hours. Another benefit of the distributed multiple site configuration is that you have less voice traffic on the WAN. A possible trade off is that you might not always be able to maximize server capacity.



Centralized multiple sites configuration

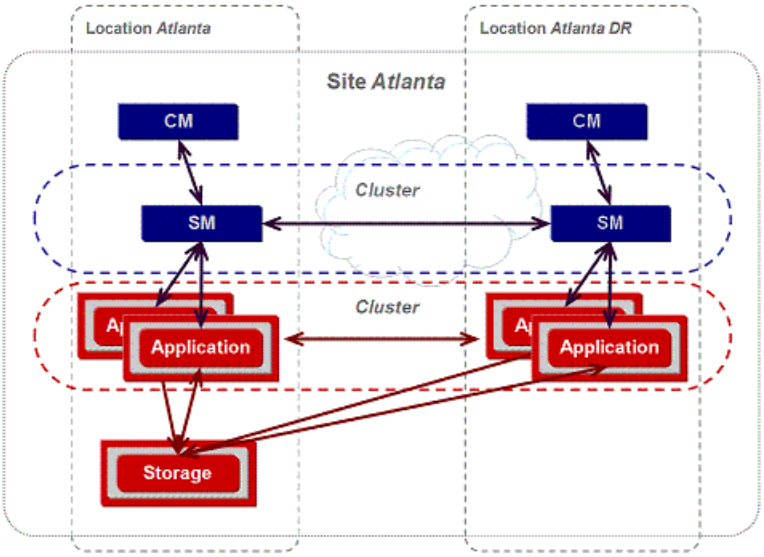
In the centralized model, Session Manager controls Communications Managers or telephony servers at all locations. The centralized configuration is a good choice if you have multiple sites and particularly, if you have sites with fewer users than the capacity of a single application server. See the following illustration for an example. You might have 8,000 users at your Atlanta site and 2,000 users at the Boston site. If you already have the telephony infrastructure in place in Boston, you can get Atlanta to handle the Boston traffic also and maximize the capacity of your servers.

Similarly, if you have a number of small offices with a couple of hundred or a thousand users at each location, each requiring only a fraction of a server, you might require significantly fewer servers than you would in a distributed configuration. By optimum utilization of the application servers, a centralized configuration lowers your total cost of ownership (TCO). The trade-off is you have more voice traffic on WAN and no local survivability.



WAN cluster Configuration

You can provide geographical redundancy by clustering application servers over WAN. Also called disaster recovery, this configuration protects you in the event of disruption of service at a location due to a network or power outage or a natural disaster. In the following illustration, the company has a redundant telephony system and redundant application servers. The degree and kind of survivability in this case depends on how much system capacity is being actively used. If Location Atlanta is running at or near 200 port capacity and the location is struck by a hurricane, the Location Atlanta DR site would take over, and there would be no loss of service. If Location Atlanta is using only 100 ports, Location Atlanta could survive a complete network or power outage at its main location, plus a failure of one of the application servers at the DR location.



Audio encoding formats

Messaging supports the following audio encoding formats:

- G.711
- Global System for Mobile Communications (GSM) 6.10

The default setting is G.711.

The audio encoding format for recording messages is administered on the System Management Interface Web pages.

G.711

G.711 audio encoding format has a coding rate of approximately 64 kbps or 8 KBps. A message that is 1 minute long requires approximately 468.8 KB of storage space when encoded using the G.711 format. One hour of G.711 requires 27.5 MB of storage space. G.711-encoded messages occupy approximately five times as much storage space as GSM 6.10.

G.711 is an international standard telephony encoding format on a 64-kbps channel. G.711 uses the Pulse Code Modulation (PCM) encoding scheme. G.711 has an 8-bit format that is used primarily for telephone quality speech. G.711 has two variants: A-law and μ-law. Typically, A-law is used in Europe, and μ-law is used in the United States. SIP integration supports both A-law and μ-law.

G.711 is the default encoding format in Messaging.

GSM 6.10

This audio encoding format has a coding rate of approximately 13 kilobits per second (kbps) or 1.6 Kilobytes per second (KBps). A message that is 1 minute long requires approximately 95.2 KB of storage space when encoded using the GSM 6.10 format. One hour of GSM 6.10 requires 5.6 MB of storage space. GSM 6.10-encoded messages occupy approximately 20% of the storage space used by G.711.

Language packs

When you install the language pack, the system checks for the available disk space on the application server. The available disk space in the application server determines the number

of languages that you can install. After you install the language pack, the languages in the pack becomes available for use.

You must always install the language packs on servers with the application role. The language packs are site specific. The list of language packs displayed by the Messaging system in User Preferences for a user is dependent on the language packs installed on the application server serving that site. If there is a cluster of application servers for a specific site, then the Messaging system retrieves the list of installed language packs from the first application server. Therefore, you must make sure that you install the same set of language packs on all cluster members.

For more information, see *Administering Avaya Aura® Messaging*.

Capacity planning

Capacity planning for an Avaya message store

The following table shows port and mailbox capacity for the standard server and the high capacity storage server, using the G.711 codec. You can use a maximum of four application servers per system. You can cluster up to three application servers for a maximum of 300 ports. You can also add a fourth application server to the cluster for redundancy as long as active traffic does not exceed 300 ports. Messaging supports 20,000 users with an Avaya message store.

While planning for the server capacity, consider that a user is the application user and a mailbox is the storage user. Each mailbox belongs to a user. As the size of the mailbox is not fixed, the mailbox number varies while the number of users remain the same.

Although you can use a high capacity storage server as a single server, this is not typical done because you will not be able to leverage the additional storage capacity in that configuration. The port capacity of the application server in the single server configuration, whether you use a standard or high capacity server, remains the same. You still have only 100 ports, and the extra storage space of the high capacity server is not used. Use of a high capacity server as a single server might prove useful if you intend to convert to a front-end/back end configuration in the future.

Port and G.711 storage capacity

Role: Hardware:	Single server (application + storage)	Application server	Storage server
Standard server	Ports: 100 User: 6,200 20 minutes. mailboxes: 8,000	Ports: 100 Users: 6,200	2,666 hours (20 min. mailboxes: 8,000) 2,759 hours (30 min. mailboxes: 5,500)

Role: Hardware:	Single server (application + storage)	Application server	Storage server
	30 minutes. mailboxes: 5,500		
High capacity storage server	Ports: 100 User: 6,200 20 minutes. mailboxes: 8,000 30 minutes. mailboxes: 5,500	—	6,666 hours (20 min. mailboxes: 20, 000) 6,750 hours (30 min. mailboxes: 13,500)

Capacity planning for third-party storage

With the Avaya Aura® Messaging flexible storage capability, you can use the Avaya message store or a third party storage destination. Messaging supports the following third-party storage destinations:

- Microsoft Exchange
- VMware Zimbra

All voice messages are stored on the user e-mail account for Exchange or Zimbra message store. Avaya message store is used to store users properties, name, and greeting recordings. Messaging supports 15,000 users with Microsoft Exchange as a storage destination.

You can retrieve only 1000 messages at any point of time from the Zimbra mailbox. The count of 1000 refers to the maximum limit for each of the Unread, Read, and Saved categories of messages. If you have 10,000 messages, that is, about 1 GB of data in your Zimbra mailbox, you must access the mailbox nine more times to retrieve all messages.

Messaging supports the G.711 and GSM 6.10 encoding formats. To determine how much space you need to allocate for message storage, use the formulas to calculate KB of disk space per minute of recorded message provided by the encoding format you choose.

Preparing your telephony server

Telephony overview

Avaya Aura® Messaging is a SIP-based messaging system. However, when coupled with a SIP gateway, Messaging supports a wide variety of analog, digital, and H323 telephony servers and telephones.

In large organizations with specialized administration roles, the switch and messaging administrators might be different individuals. If this is true for your organization, you may need

to coordinate integration activities because some telephony parameters must be identical on the telephony and application servers.

Configuration Notes

Avaya provides Configuration Notes with switch-specific configuration information. You can download these Configuration Notes from the Avaya Support Web site at http://www.avaya.com/support.

Resource management

Ensure that your telephony server has sufficient resources dedicated to the messaging functionality. The variables for calculating capacity and determining the number of SIP trunks to dedicate to Messaging are:

- The amount of network traffic that flows through your messaging system
- The number of ports reserved for messaging
- The types of telephones your organization uses

Bandwidth utilization between the Messaging servers

To obtain an estimate of the additional traffic the Messaging system will add to your network, you can calculate the bandwidth usage between the application servers and the storage server. The calculation must include the number of application servers in the Messaging system, the number of ports on each application server, and usage characteristics. The encoding method you use is also a key factor.

For a worst case estimate of network load added by a Messaging system using the G.711 encoding format, which has a bit rate of 64 kbps, the formula is:

number of servers X the number of ports on each server X 64

For a site with a Messaging system containing three application servers, each with 100 ports, the formula is:

3 X 100 X 64 = 19,200 kbps

If you use the GSM 6.10 encoding format, which has a bit rate of 13 kbps, the calculation for this site yields the following:

3 X 100 X 13 = 3,900 kbps

This calculation is based on the assumption that all ports are recording or playing voice data at the same time. Note that this formula estimates the total network traffic potentially added but does not indicate how many ports receive calls and how many ports make calls. To allow for the overhead used by the network protocols and options, add 10% to the result. Note that

this worst case network load calculation does not include burst rates caused by bursty message deliveries or bursty message playback.

Systems with multiple sites

Each Messaging site has a one-to-one relationship with a telephony server. If your organization uses more than one telephony server, then the organization has a multisite messaging system. You must repeat administration activities on each telephony server in your telephony network.

Role of Message Networking in Avaya Aura® Messaging

You do not need Message Networking to network multiple Avaya Aura® Messaging systems. You can optionally use Message Networking as an LDAP server database to update the local and remote user database and to perform user lookup. Messaging Networking does not have any role in delivering the messages if messages are sent from Avaya Aura® Messaging to Avaya Aura® Messaging.

Message Networking is required when you network the messaging systems like Audix, Aria, and other legacy systems to the Avaya Aura® Messaging system. To network with the traditional voice messaging systems, Avaya Aura® Messaging uses Message Networking. Message Networking not only updates the user database and performs the user lookup but also delivers the messages.

Avaya Aura® Messaging supports a maximum of 100,000 remote users, irrespective of whether Message Networking is used to connect the Avaya Aura® Messaging system to other messaging systems.

E.164 Dial Plan

Messaging supports full E.164 mailbox numbers in the system. Administrators can configure mailbox numbers without using the full E.164 number and map these mailbox numbers to a full E.164 number. Therefore, users at any site can continue to use mailbox numbers locally that are smaller in length but are still uniquely identifiable in the local context.

Messaging supports only the fixed mailbox number length system wide. Messaging does not support variable length mailbox numbers.

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

Licensing

Avaya controls the use and access to some Messaging features through licenses, which the customer must purchase, including the number of Messaging enabled mailboxes the customer wants to use.

Messaging uses Web License Manager (WebLM) as its standard licensing mechanism. Messaging features are tied to the WebLM server and any client of the server can acquire and use a licensed feature. Messaging requires a WebLM hosted license. Messaging uses an enterprise license that allows the same license to be shared with multiple Messaging systems within an organization, if desired. The number of seat licenses is shared between all the Messaging systems associated with the license.

The license file controls the number of user mailboxes. The license is created based upon the host ID of the WebLM server. The user count can only be changed through PLDS either by purchasing additional seats or by moving seats between licenses. If more than one Messaging system exists in an enterprise, then the licensing model should be planned before obtaining the required license through PLDS.

WebLM Server

A WebLM server is installed as part of the System Platform installation and will be automatically configured as the WebLM server to be used by Messaging. Customers can subsequently change this configuration if the customers already have a centralized WebLM server that the customers would prefer to use instead.

In larger or more complex environments, customers may have multiple Messaging systems. Each Messaging system can be associated with just one license file and therefore, consideration must be given to how the licenses will be distributed. In many cases, these decisions should be made before the license is obtained through PLDS.

Mailbox licensing

Messaging offers two mailbox licenses: Mainstream and Basic. The Mainstream license is the full featured Messaging system that includes Reach Me, Notify Me, and Speech based addressing features, plus fax support and IMAP access to the Avaya message store. The Basic license provides a subset of the Mainstream features. Administrators can mix Mainstream and Basic licenses system wide and also on individual locations.

Administrators control the features that are included in the mainstream license through Class of Service (CoS). A user in a CoS that includes one or more mainstream features requires a mainstream license. Licensing and CoS controls access to the features. User Preferences

takes into account what features a user has access to and only displays options and settings for those feature that a user can use.

Removing a feature from a user CoS or moving a user to a CoS with fewer features affects the feature availability in two different ways, depending on whether the feature is actively enabled by the user or passively available to the user.

The Reach Me, Notify Me, and Fax features function even when these features are removed from a user CoS, as these features are actively enabled by users. However, the user cannot change the settings for these features in the User Preferences Web pages once these features are removed from a user CoS.

The IMAP access to Avaya message store and Speech-based message addressing features are passively enabled for users in a CoS with these features. The user does not have control over these features. When these features are removed from a user CoS, these features immediately stop functioning.

Feature set comparison

The mainstream license is required for the following features only:

- Reach Me
- Notify Me
    - Text message or page notification
    - Phone call to a telephone or mobile phone
    - E-mail copy
- Fax
    - Detect and transfer to fax server
    - Receive and forward to e-mail
- IMAP access to the Avaya message store
- Speech based features
    - Speech recognition for addressing
    - Basic Speech Auto Attendant
    - Access to Avaya one-X® Speech

Except the listed features, all other features of the Messaging system do not require a mainstream license.

Information mailbox licensing

Messaging does not require a mailbox license for Caller Applications and information mailboxes.

You can assign the Info Mailbox CoS to each user to create a message for an information mailbox. A typical informational message includes details about directions, business hours, weather, or human resources information. You can record messages for an information mailbox that take up to 5 minutes to play.

Server specifications

The following servers support Messaging.

Table 1: Dell™ PowerEdge™ R610 Server

Name of the component	Standard Server	High Capacity Storage Server
Chassis	1U	1U
Processor speed	E5620 2.4 Ghz 4-core	E5620 2.4 Ghz 4-core
Number of processors	1	1
System memory	12 GB	12 GB
Ethernet ports	2	2
RAID type	RAID 5	RAID 5
Disk	3 x 146 GB 10k	4 x 146 GB 10k
Standard power supply	1 x 502 W	2 x 502 W

Table 2: HP ProLiant DL360 G7 Server

Name of the component	Standard Server	High Capacity Storage Server
Chassis	1U	1U
Processor speed	E5620 2.4 Ghz 4-core	E5620 2.4 Ghz 4-core
Number of processors	1	1
System memory	12 GB	12 GB
Ethernet ports	2	2

Name of the component	Standard Server	High Capacity Storage Server
RAID type	RAID 5	RAID 5
Disk	3 x 146 GB 10k	4 x 146 GB 10k
Standard power supply	1 x 460 W	2 x 460 W

Table 3: S8800 Server

Name of the component	Standard Server	High Capacity Storage Server
Chassis	1U	1U
Processor speed	E5520 Quad-core 2.26 Ghz processor	E5520 Quad-core 2.26 Ghz processor
Number of processors	1	1
System memory	12 GB	12 GB
Ethernet ports	2	2
RAID type	RAID 5	RAID 5
Disk	3 x 146 GB 10k rpm SAS hard disk drives	4 x 146 GB 15k rpm SAS hard disk drives
Standard power supply	Single power supply	Dual power supplies

Table 4: S8730 Server

Name of the component	Standard Server	High Capacity Storage Server
Processor speed	AMD 2352 QUAD core processor	AMD 2352 QUAD core processor
System memory	12 GB	12 GB
Ethernet ports	2	2
RAID type	RAID 5	RAID 5
Disk	3 x 146 GB 15k 2.5 inch SAS hot-plug hard disk drives	4 x 146 GB 15k 2.5 inch SAS hot-plug hard disk drives
Standard power supply	800 Watt, CE Mark Compliant hot-plug power supply	800 Watt, CE Mark Compliant hot-plug power supply Additional hot-plug redundant power supply

Hardware requirements

Customer-provided equipment

The customer must provide the following equipment:

- Standard 19-inch four-post equipment rack that is properly installed and secured. The rack must meet the following standards:
  - American National Standards Institute and Electronic Industries Association standard ANSI/EIA-310–D-92
  - International Electrotechnical Commission standard IEC 297
  - Deutsche Industrie Norm standard DIN 41494
- Screws that come with the racks for installing the rails.
- #2 cross-point (Phillips) screwdriver or 3/8 inch flathead screwdriver.
- USB keyboard, USB mouse, and monitor must be available on the site for advanced installation or troubleshooting.
- Power from a nonswitched electrical outlet.
- Access to the network.

Software requirements

Required software for Messaging

The following table lists the Web browser requirements for the Messaging system.

Software	Supported versions
System Platform	Internet Explorer 7 Mozilla Firefox 2 Mozilla Firefox 3
User Preferences System Management Interface	Internet Explorer 7 Internet Explorer 8 Mozilla Firefox 3.5 Safari 4

The following table lists the software requirements for the Messaging system.

Software	Supported versions
System Platform	6.0.0.0.11
Messaging	6.0

You must install Communication Manager patches because Messaging uses the Communication Manager platform that requires software updates.

The following table lists the supported versions of Microsoft Outlook.

Software	Supported versions
Microsoft Outlook	• 2003 • 2007 • 2010

Supported versions of Avaya products

The following table lists the supported versions of the Avaya products.

Software	Supported versions
Avaya Aura® SIP Enablement Services	5.2.1
Avaya Aura® Session Manager	6.0
Message Networking	5.2
Avaya one-X® Speech	5.2
Avaya one-X® Mobile	5.2 6.0
Avaya one-X® Communicator	5.2 6.0
Avaya Aura® Communication Manager	5.2.1 6.0.1

Supported versions of third-party software

Avaya supports the use of the documented software versions with the current release of Messaging. These software versions are the minimum versions that Avaya requires.

This release does not support operating systems, databases, Web servers, switches, or other software platforms that are not documented here, unless stated otherwise in a Product Support Notice.

Avaya will support subsequent updates and service packs that provide corrections for a bug, defect, or problem for the documented software versions. The support depends on the following:

- The manufacturer must guarantee that the updates and service packs are backwards compatible with the supported versions.
- The updates and service packs do not include changes to the core functionality or new features.

Note:

Before you apply the updates and service packs to a production environment, you must test all updates and service packs that follow the supported versions in a development environment.

Security requirements

Before implementing a Messaging system, ensure that the customer security staff reviews and approves the Messaging deployment. Customers should engage the expertise of their security staff early in the implementation process. The security staff must consider how the security staff will incorporate the Messaging system into their routine maintenance of virus protection, patches, and service packs.

Additional security information

For additional security information and documentation on all Avaya products, see the Avaya Security Advisories Web site at http://support.avaya.com/security. The Web site includes information on the following topics:

- Avaya Product Security Vulnerability Response Policy
- Avaya Security Vulnerability Classification
- Security advisories for Avaya products
- Software patches for security issues
- Reporting a security vulnerability
- Automatic e-mail notifications of security advisories

For additional information about security practices, see the National Security Agency Security Configuration Guides at http://www.nsa.gov/snac.

Traffic flow

Your IT infrastructure needs to allow network traffic to move freely to and from the Messaging system. The following tables lists services used by Avaya Aura® Messaging, and associated protocol and port number.

For the System Platform ports, see *Administering Avaya Aura® System Platform* on the Avaya Support Web site at http://support.avaya.com/css/Products/P0585.

Some considerations for using the following tables:

- Direction:
  - Inbound: The port is open for external access to the server.
  - Outbound: The server transmits data externally over the port.
- Configure: The port value can be changed by the customer from the SMI.
- Enable/Disable: The port can be enabled and disabled by the customer from the SMI.
- Server type: Application server, Storage server, or both.
- X: The service or option is available.

Table 5: LAN ports used by Messaging servers

Service name	Protocol	Port	Direction	Configure	Enable/ Disable	Server type	Notes
ftp	TCP	21	Both		X	Both	
ssh	TCP	22	Both		X	Both	
telnet	TCP	23	Both		X	Both	
smtp	TCP	25	Both	X	X	Both	
dns	UDP	53	Outbound			Both	
http	TCP	80	Inbound			Both	Redirects to HTTPS by default.
pop3	TCP	110	Inbound	X	X	Both	
ntp	TCP	123	Outbound			Both	
imap	TCP	143	Inbound	X	X	Both	
snmp	UDP	161	Both			Both	
snmptrap	UDP	162	Both			Both	
ldap	TCP	389	Inbound	X		Both	

Service name	Protocol	Port	Direction	Configure	Enable/ Disable	Server type	Notes
http	TCP	443	Inbound			Both	
smtps	TCP	465	Both	X	X	Both	
syslog	TCP	514	Inbound			Both	
ldaps	TCP	636	Both	X	X	Both	
imaps	TCP	993	Inbound	X	X	Both	
pop3s	TCP	995	Inbound	X	X	Both	
hp-sshd	TCP	2222	Inbound		X	Both	
h248-binary	TCP	2945	Inbound			Both	
secure-sat	TCP	5022	Inbound		X	Both	Avaya proprietary use (unused) - secure System Access Terminal.
sat	TCP	5023	Inbound		X	Both	Avaya proprietary use (unused) - secure System Access Terminal.
sip	TCP	5060	Both	X		Application	
sip tls	TCP	5061	Both	X		Application	
speechifyTTS	TCP	5555	Inbound			Both	Avaya proprietary use - Used to translate text to speech.
java-aic	TCP	7117	Inbound			Both	Avaya proprietary use - AxC.
java-mwilistener	TCP	7121	Inbound			Both	Avaya proprietary use - MWI Listener.

Service name	Protocol	Port	Direction	Configure	Enable/ Disable	Server type	Notes
java-aicweb	TCP	7171	Inbound			Both	Avaya proprietary use - AxC web server.
adcs—jax	TCP	8081	Both			Both	Avaya proprietary use.
adcs—fetch	TCP	8083	Both			Both	Avaya proprietary use - cluster communications.
N/A	UDP	1024-65534	Outbound			Application	Used by several protocols to reach clients, including RTP/SRTP.
mcapi	TCP	55000	Both	X		Both	Avaya proprietary use - legacy mail access API.
N/A	ICMP		Both			Both	Used for *ping* support.

Table 6: LAN ports used by Messaging adjuncts

Service Name	Protocol	Port	Inbound/ Outbound	Message Networking	Avaya one-X® Speech	Avaya one-X® Mobile	Avaya one-X® Portal
ftp	TCP	21	Both				
ssh	TCP	22	Both				
telnet	TCP	23	Both				
smtp	TCP	25	Both	X	X	X	X
dns	UDP	53	Outbound				
http	TCP	80	Inbound				

Service Name	Protocol	Port	Inbound/ Outbound	Message Networking	Avaya one-X® Speech	Avaya one-X® Mobile	Avaya one-X® Portal
pop3	TCP	110	Inbound				
ntp	TCP	123	Outbound				
imap	TCP	143	Inbound		X	X	X
snmp	UDP	161	Both				
snmptrap	UDP	162	Both				
ldap	TCP	389	Inbound	X	X	X	X
http	TCP	443	Inbound				
smtps	TCP	465	Both	X		X	X
syslog	UDP	514	Inbound				
ldaps	TCP	636	Both	X			X
imaps	TCP	993	Inbound			X	X
pop3s	TCP	995	Inbound				
hp-sshd	TCP	2222	Inbound				
h248-binary	TCP	2945	Inbound				
secure-sat	TCP	5022	Inbound				
sat	TCP	5023	Inbound				
sip	TCP	5060	Both				
sip tls	TCP	5061	Both				
speechifyTTS	TCP	5555	Inbound				
java-aic	TCP	7117	Inbound				
java-mwilistener	TCP	7121	Inbound				
java-aicweb	TCP	7171	Inbound				
adcs—jax	TCP	8081	Both				
adcs—fetch	TCP	8083	Both				

Service Name	Protocol	Port	Inbound/ Outbound	Message Networking	Avaya one-X® Speech	Avaya one-X® Mobile	Avaya one-X® Portal
N/A	UDP	1024-65534	Outbound				
mcapi	TCP	55000	Both				
N/A	ICMP		Both				

Index

L

M

N

O

P

R

S

T

U

W

Z