



Installing Avaya Modular Messaging on a Single Server Configuration

August 2011

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](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 type(s)

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

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: Introduction.....	9
Purpose of this document.....	9
Avaya Modular Messaging.....	9
Avaya Aura® System Platform.....	10
License requirements.....	12
Remote accessibility and alarming.....	12
Security considerations.....	13
Installation checklist.....	14
Chapter 2: Installation prerequisites.....	17
Overview.....	17
System specifications.....	17
HP DL360 G7 Server specifications.....	17
Pre-installation tasks.....	19
Download required documents.....	19
Pre-installation data gathering.....	19
Obtain a Modular Messaging template.....	20
Install System Platform.....	20
Configure SAL.....	21
Configure the network settings.....	22
Date and time configuration.....	22
Configure PBX.....	22
Preparing for installation.....	23
Registering for PLDS.....	24
Copying template from optical media to the System Platform server.....	24
Corporate Windows domain requirements.....	25
Creating user accounts in the corporate Windows domain.....	25
Creating computer accounts in the corporate Windows domain.....	26
Chapter 3: Configuring the SAL Gateway and System Registration.....	29
Registering the system.....	29
Adding managed devices to the SAL Gateway.....	30
Chapter 4: Accessing the System.....	33
Accessing the System.....	33
Accessing the System Domain (Dom0).....	33
Accessing the Console Domain (CDOM).....	34
Accessing the MSS using the MSS Web console.....	35
Accessing the MAS using RDC.....	35
Accessing the Web Client server using RDC.....	36
Chapter 5: Installing Avaya Modular Messaging.....	37
Overview.....	37
Locating templates.....	38
Selecting the Modular Messaging template.....	39
Customizing the template.....	39
Configuring the Modular Messaging template.....	40
Setting up the network.....	41

Setting up the Modular Messaging network.....	41
Setting up the Windows domain configuration.....	42
Configuring Modular Messaging.....	43
Creating Modular Messaging accounts.....	43
Configuring the switch integration.....	44
Saving the configuration.....	45
Verifying the installation.....	46
Chapter 6: Configuring Modular Messaging.....	47
Overview.....	47
Adding the MSS as a trusted site.....	47
Preparing the MAS.....	48
Activating Microsoft Windows.....	48
Updating Microsoft Windows.....	49
Installing and administering anti-virus software.....	50
Configuring licenses.....	50
License management.....	50
Obtaining licenses.....	51
Applying license file on the WebLM server.....	52
Importing certificates from license.....	52
Verifying the WebLM URL in VMSC.....	53
Entering Product ID for the MAS.....	53
Configure specific features on an MAS.....	54
Configuring specific features as needed.....	54
Configuring Call Me service.....	55
Configuring Notify Me.....	55
Configuring MWI service.....	55
Configuring MM Audit Service.....	56
Configuring the MM Fax Sender server.....	57
Configuring languages and multi-lingual TTS.....	61
Configuring offline access to messages.....	62
Chapter 7: Updating Modular Messaging.....	63
Overview.....	63
Downloading software updates.....	63
Copying software updates to the MAS.....	63
Installing software updates on the MAS.....	64
Verifying software updates on the MAS.....	66
Installing software updates on the MSS.....	66
Installing software updates on the Web Client server.....	67
Chapter 8: Performing acceptance tests for a new installation.....	69
Adding test subscribers.....	69
Running acceptance tests.....	71
Leaving a call answer message.....	71
Retrieving test messages in integrated mode.....	72
Creating and sending a test message in non-integrated mode.....	74
Testing the outcalling capability.....	75
Creating and printing a fax message.....	77
Removing the test subscribers on the MSS.....	78

Chapter 9: Setting up alarming.....	81
Configuring the system alarms.....	81
Setup alarming on the MSS.....	81
Specifying MSS alarm origination.....	82
Configuring serviceability settings on MAS.....	83
Testing alarming origination.....	83
Chapter 10: Creating snapshot of the MAS.....	85
Taking snapshot of the MAS.....	85
Restoring the MAS from the snapshot.....	86
Chapter 11: Backing up the system.....	87
Backing up the system.....	87
Using the DCT to analyze the current configuration.....	88
Checking the spool folder on the MAS.....	89
Running backups on the MAS.....	89
Restoring backed-up MAS data.....	90
Backing up the MSS.....	92
Chapter 12: Restoring the system.....	95
Recovering the system.....	95
Restoring data on the MSS.....	96
Restarting the messaging services.....	98
Completing VMSC setup.....	100
Completing MSS administration.....	100
Restoring backed-up MAS data.....	101
Restoring Caller Applications.....	103
Chapter 13: Troubleshooting.....	105
Template installation summary shows errors.....	105
Insufficient resources to install the template.....	105
Template installation complete but there are lines in the template installation log, which says 'with problem finished mss configuration'.....	106
Template installation completed but last status message says mas: ConfigCredentialLDAP FAILED.....	106
System Platform Web Console does not update information for long time.....	107
How to know if the configuration was successful?.....	107
Appendix A: Planning form for installing Modular Messaging.....	109
Appendix B: Field descriptions of planning form for installing Modular Messaging... 	113
Corporate Network Details field descriptions.....	113
Domain Name Servers field descriptions.....	113
Corporate MM networking field descriptions.....	114
Windows Domain field descriptions.....	115
Modular Messaging Configuration field descriptions.....	115
Modular Messaging Accounts field descriptions.....	116
Switch Integration Information field descriptions.....	118
Appendix C: Alternative methods for preparing the installation source.....	119
Setting up the HTTP server.....	119
Setting up a USB flash drive.....	120
Appendix D: Alternative methods of accessing the system.....	123
Accessing the MAS using the VNC viewer installed on the System Platform.....	123
Accessing the MAS using the VNC viewer from a remote computer.....	123

Accessing the MSS using PuTTY.....	124
Accessing the MSS using virsh console command through PuTTY.....	125
Glossary.....	127
Index.....	133

Chapter 1: Introduction

Purpose of this document

This guide provides information about installing the Avaya Modular Messaging on a single server configuration. You must have installed Avaya Aura[®] System Platform before installing Modular Messaging. This guide helps you with the following:

- Installing and configuring Avaya Modular Messaging
- Testing and backing up the Modular Messaging system
- Troubleshooting Avaya Modular Messaging

Avaya Modular Messaging

You can install Modular Messaging Release 5.2 on a single server for Message Storage Server (MSS) systems. This single server hosts both the MSS and the MAS. The Web Client and Web Subscriber Options server can also run on the same single server. Single server configuration uses System Platform to provide the virtualization of the server and simplifies the installation of Modular Messaging. With the single server configuration, you can do installations, upgrades, and updates of Modular Messaging remotely, thus removing the need for onsite implementations. System Platform makes remote installation possible using Secure Access Link (SAL).

Avaya offers product-specific templates to install different products on a System Platform. A template is a definition of a set of one or more applications to be installed on the System Platform. Depending on the template that you purchased, you get one of the following templates:

- `modular_messaging.ovf`: To install the pre-configured images of one MSS and one MAS.
- `wcwo_mm.ovf`: To install the pre-configured images of one MSS, one MAS, and a combined Web Client and Web Subscriber Options server.

You can obtain these templates from the Product Licensing and Delivery System (PLDS) or Avaya-provided optical media (CD/DVD) before installing the Modular Messaging software.

PLDS allows Avaya customers, Partners, and associates to manage software licensing and to download software for various Avaya products.

You can verify and re-configure the template parameters, including network and server details and the Modular Messaging-specific parameters, using the System Platform pre-installation Web page. You can also prepare an Electronic Pre-installation Worksheet (EPW) file ahead of time so that the values required during the actual installation are readily available. The installation wizard is embedded within the template that enables you to upload an existing EPW file. If you do not already have a valid EPW file, the wizard enables you to create one during the installation of the template. For descriptions of the fields in the EPW file, see Appendix B: Field descriptions of planning form for installing Modular Messaging.

 **Note:**

You must have installed System Platform before installing Modular Messaging.

Single server configuration supports the following:

- 48 ports
- Up to 2,500 subscribers
- Maximum 250,000 remote networked subscribers
- SIP integration
- SAL 1.5 for alarming and remote access
- LAN-based backup, administrators can back up data to a remote storage location on the LAN through FTP and SFTP. Customers need to provide a FTP or SFTP server for the backups. For more information, see *Avaya Modular Messaging Concepts and Planning Guide*
- Web based console for easy maintenance of the system

Avaya Aura[®] System Platform

The System Platform is a generic virtual server software platform that provides a common set of features and services that allow pre-installed and configured virtual applications, called solution templates, to co-reside on a single physical server.

System Platform is a Xen-based platform that includes a

- Base CentOS 5.2 Linux system running the Xen hypervisor (dom 0)
- Web-based management console for installing and managing templates
- Virtual machine for System Platform system utilities

System Platform features include the following:

- Secure Access Link (SAL) that handles alarming and remote access
- Patches and upgrades that use a consistent upgrade method for all products in the solution template
- Security that conforms to Avaya product security standards
- A WebLM server for managing product licenses
- A Network Time Protocol (NTP) clock sync to a customer provided NTP server

Virtual Machines

System Platform includes a base operating system (CentOS 5.2), the Xen Hypervisor, and a virtual machine (CDOM) that is used to manage the platform.

- System Domain (Dom-0): In addition to exporting virtualized instances of CPU, memory, network and block devices, Xen exposes a control interface to manage how these resources are shared between the running domains. Access to the control interface is restricted to one 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.
 - Common logging and alarming
 - Remote access
 - System Platform Web Console
 - Upgrades and patches
 - WatchDog
 - Licensing

Template

System Platform makes remote installation possible using product-specific templates. A template is a definition of a set of one or more applications to be installed on System Platform. Templates are XML files that are compatible with the Open Virtualization Format (OVF) standard. A System Platform template describes a set of virtual machines intended to be installed and run together as one offer bundle, called a virtual appliance in the OVF specification.

Following is the composition of template:

- Virtual Appliance
- Plug-ins
- Pre-install scripts
- Post-install scripts
- OVF descriptor

License requirements

Modular Messaging uses WebLM as its standard licensing mechanism. WebLM is a Web-based licensing solution that facilitates license management. Using WebLM, an administrator can track and manage licenses of multiple Avaya software products installed in an organization from a single location. To track and manage licenses of an Avaya software product, installed in an organization, WebLM requires a license file for the product. The license file contains information about the product, major release, the licensed features of the product, and the licensed capacities of each feature bought by your organization.

Avaya provides the licenses through the PLDS (<https://plds.avaya.com>). With the single server configuration, 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 Modular Messaging. Customers can subsequently change this configuration if they already have a centralized WebLM server that they would prefer to use instead or they choose to install the WebLM on a standalone server.

For more information, see *Installing and configuring Avaya WebLM server*.

Remote accessibility and alarming

Single server configuration uses Secure Access Link (SAL) gateway to manage alarming and remote access.

SAL provides support and remote management of a variety of devices and products. SAL provides:

- Remote access to support personnel for accessing supported devices
- A user interface to configure SAL interfaces to managed devices, Concentrator Remote and Core Servers, and other settings
- Redundancy in gateways for enhanced service availability
- Diagnostic facilities that ensure that all gateway components operate as required

System Platform installation includes the following SAL agents that you can use for alarming and remote access.

- SAL Agent for remote access: The SAL Agent installed on the System Platform provides network based remote access to Avaya Services. Use of this remote access mechanism is largely transparent to the Modular Messaging system running on System Platform, although you need to make sure Services knows the access mechanisms required for the

application. You also need to provide Modular Messaging product ID (or alarm ID) and solution element ID.

- SAL Agent for alarming: System Platform runs a SAL Agent capable of sending alarms via HTTPS to Avaya Services and/or via Simple Network Management Protocol (SNMP) to the customer's Network Management System (NMS).

You must configure and register SAL before installing Modular Messaging. Avaya Partners and customers need to ensure that SAL is configured and registered properly. Avaya support will be delayed or not possible if SAL is not properly implemented.

The System Platform Web Console includes a link to the SAL Gateway Management Portal where you can configure alarms settings.

Security considerations

You must consider the following security-related issues while installing Modular Messaging.

On-site security considerations

On-site installers must take precautions to protect passwords and restrict access to the system.

Password security protection

To protect password security:

- Do not leave written passwords lying out or allow anyone to see the passwords.
- At the first opportunity, give the passwords directly to the designated customer representative.
- If you suspect that the security of the system was compromised, notify the project manager or the system administrator.

System security protection during installation

To protect system security during the installation:


- Remove all test subscribers and test mailboxes from the system when the procedures instruct you.
- Do not configure any unassigned mailboxes. Unassigned mailboxes are mailboxes that have an extension, but no subscriber assignment.
- Always log off or lock the server if you leave it unattended, even for a short period.



Ongoing system security considerations


Customers must obtain and install the anti-virus software on any Microsoft Windows computer that is to run Avaya Modular Messaging software. Customers must also routinely install updates for Microsoft Windows systems to protect the system from known security weaknesses. Updates include operating system updates and security patches. For more

information, obtain *Modular Messaging and security* from the Avaya Support Web site (<http://www.avaya.com/support>).

Installation checklist

Use the following checklist to install the Avaya Modular Messaging. As you complete a task, make a check mark in the  column.

#	Task	Notes	
 Note: Steps 1 - 11 can be performed by the customer, their Avaya-certified business partner or contractor, or an Avaya technician if the customer has purchased that option.			
Installation prerequisites			
1	Download required documentation. See Download required documents on page 19.		
2	Gather pre-installation data. See Pre-installation data gathering on page 19.		
3	Obtain Modular Messaging template. See Obtain a Modular Messaging template on page 20.		
4	Verify that all equipment is on site.	Compare the inventory list of hardware and components that you ordered to the contents of the shipping boxes; do not rely on the packing slip for correct information. If you found any discrepancy between the inventory list and the contents of the shipping boxes, immediately inform Avaya.	
5	Install the System Platform, configure the IP address and set the password. See Install System Platform on page 20.		
6	Configure network.		

#	Task	Notes	✓
	See Configure the network settings on page 22.		
7	Configure date and time. See Date and time configuration on page 22.		
8	Configure PBX. See Configure PBX on page 22.		
9	Prepare for the installation. See Preparing for installation on page 23.		
10	Create user accounts and computer accounts in the corporate Windows domain. See Corporate Windows domain requirements on page 25.		
Configure remote accessibility			
11	Register the system and configure the SAL Gateway. See <ul style="list-style-type: none"> • Registering the system on page 29 • Adding managed devices to the SAL Gateway on page 30. 		
 Note: Step 12 onwards must be performed by either a certified Avaya Partner or Avaya technician. However, customer involvement will be required for some tasks.			
Install Modular Messaging			
12	Use the System Platform Web Console to install Modular Messaging. See Chapter 5: Installing Avaya Modular Messaging.		
Configure Modular Messaging			
13	Activate MS Windows OS. See Activating Microsoft Windows on page 48.		
14	Update Microsoft Windows. See Updating Microsoft Windows on page 49.		
15	Install and administer anti-virus software.		

#	Task	Notes	✓
	See Installing and administering anti-virus software on page 50.		
16	Configure licenses. See License management on page 50.		
17	Enter Product ID for the MAS. See Entering Product ID for the MAS on page 53.		
18	Configure specific features. See Configuring specific features as needed on page 54.		
Completing installation			
19	Update Modular Messaging. See Overview on page 63.		
20	Perform acceptance testing of the system. See Performing acceptance tests for a new installation on page 69.		
21	Setup alarming on the MSS. See <ul style="list-style-type: none"> • Configuring the system alarms on page 81. • Setup alarming on the MSS on page 81. 		
22	Create snapshot of the MAS. See Taking snapshot of the MAS on page 85.		
23	Back up the system. See Backing up the system on page 87.		

Chapter 2: Installation prerequisites

Overview

This chapter describes the prerequisites that must be met before you can install Modular Messaging.

System specifications

S8800 1U Server specifications

Single server configuration supports S8800 1U server. These servers arrive at your site with all appropriate components and memory. You do not need to add anything to the servers on site. The following table lists the specification of the S8800 1U server.

Component	Description
Chassis	1U
Processor Speed	2.26GHz-E5520
Number of Processors	2 processors with 4 cores each
Total Memory in GB	12 GB
Ethernet Ports	2
RAID Type	RAID 5
Disk	5 x 146Gb 10k rpm SAS hard disk drives
Standard Power Supply	Dual power supplies

HP DL360 G7 Server specifications

Base unit	Baseline	Options
DL360 G7	1U chassis, dual socket	No additional options supported.

Installation prerequisites

Base unit	Baseline	Options
Processor	Intel E5620 Quad Core /2.4 GHz (Westmere) 3 memory channels per CPU with up to 3 RDIMMs per channel (most applications use 1 or 2 RDIMMs per channel to optimize memory speed)	<ul style="list-style-type: none"> • Intel X5670 six Core/2.93 GHz (Westmere) • Upgradable to dual processors for either E5620 or X5670
Memory	2 GB DDR3 RDIMMs (1333 MHz)	4 GB DDR3 RDIMMs (1333 MHz)
HW RAID 1	P410i RAID controller with 256MB cache and battery backup. Optioned as RAID 1 or 5	N/A
Hot-Plug disk drive cage	4 Small Form Factor 2.5" hot-plug hard drives bays are available when an optical drive is installed.	HP offers servers with 8 drive bays that do not support an optical drive (not supported by Avaya).
Disk drive	146GB SAS 2.5" 10K RPM 6G DP Hard Drive. Two base configurations: <ul style="list-style-type: none"> • 136 total: RAID 1, 2 x 146GB drives • 272 total: RAID 5, 3 x 146GB drives 	Options: <ul style="list-style-type: none"> • Additional 146GB 10K RPM drive (4 max. with optical drive) • High performance 146GB 15K drives • 300GB 10K HDD
NICs	4 integrated ENET Gigabit NIC ports with TCP offload engine (included on motherboard)	HP NC382T PCI Express Dual Port Gigabit NIC expansion card (Broadcom 5709 silicon)
PCI slots	Two PCI-Express Gen 2 expansion slots: (1) full-length, full-height slot and (1) low-profile slot (1-FL/FH x 16 PCIe & 1-LP x 8 PCIe Riser	Meeting Exchange Recording uses a PCI-X riser in place of the low profile PCIe riser in the standard server.
Removable media	Slim line SATA DVD-RW optical drive (used in all Avaya configurations)	No additional options supported.
Power supply	460 W hotplug AC power supply	<ul style="list-style-type: none"> • 750W AC power supply • 1200W DC power supply • Single and dual power supply configurations
Fans	3 fan modules (fan redundancy standard)	No additional options supported.
Additional items	1 front USB, 2 back USB, 1 internal USB	

Pre-installation tasks

Download required documents

You can download and use the documentation described in this section to install Modular Messaging. You can obtain this information from the Avaya Support Web site. Always check the Avaya Support Web site at <http://www.avaya.com/support> for the latest updates and information before you install or upgrade Avaya products. Note that links and paths on the Avaya Support Web site might change.

- Modular Messaging Concepts and Planning Guide
- Installing and Configuring Avaya Aura® System Platform
- Administering Avaya Aura® System Platform
- Modular Messaging for the Avaya Message Storage Server (MSS) Installation and Upgrades
- Messaging Application Server Administration Guide for Avaya Modular Messaging with the Avaya MAS and MSS
- Avaya Modular Messaging Documentation Library
- Configuration notes
- MSS alarms
- Installing and Configuring Avaya WebLM server
- Getting Started with Avaya PLDS
- Secure Access Link 1.5 SAL Gateway Implementation

Pre-installation data gathering

While installing and configuring Avaya Modular Messaging you are required to fill in several fields. Having the information available ahead of time, makes the installation faster and accurate.

To ensure that you have gathered all the required data before the actual installation, fill out the [Planning form for installing Modular Messaging](#) on page 109.

Obtain a Modular Messaging template

You can obtain the Modular Messaging template from:

- Avaya-provided optical media (CD/DVDs). When you purchase the product, Avaya provides you one template CD (*modular_messaging.ovf* or *wcwo_mm.ovf*) and 2 application DVDs.
- The Product Licensing and Delivery System (<https://plds.avaya.com>) Web site. Download the .iso files and burn them onto Dual Layer DVDs. For more information on accessing and downloading the files from PLDS, see *Getting Started with Avaya PLDS* available on <http://www.avaya.com/support>.

The following describes the content of the optical media:

- **Modular Messaging single server configuration Template MAS/MSS**

modular_messaging.ovf: MAS, MSS configuration (Modular Messaging without Web Client server)

- **Modular Messaging single server configuration Template MAS/MSS/Web Client/WSO**

wcwo_mm.ovf: MAS, MSS, and WC/WSO configuration (Modular Messaging with Web Client server)

- **Modular Messaging single server configuration Application (DVD 1 of 2)**

- Compressed disk image for MSS (**.gz file*)
- Compressed disk image for Web Client (**.gz file*)
- Manifest file (*.mf file*)
- Pre-installation Web app (*mmpreconfig.war*)
- Plug-in scripts

- **Modular Messaging single server configuration Application (DVD 2 of 2)**

Compressed disk image for MAS (**.gz file*)

Install System Platform

You must have installed System Platform before installing Modular Messaging.

Modular Messaging on a single server configuration with the HP DL360 G7 server supports System Platform 6.0.3.0.3.

Modular Messaging on a single server configuration with the S8800 server supports System Platform 1.1.0.0.10 and 6.0.3.0.3.

Existing customers upgrading to System Platform 6.0.3.0.3 must apply Service Pack 1.1.1.97.2 patch prior to the upgrade. For information on upgrading System Platform, see the *Upgrading Avaya Aura® System Platform* guide available on the Avaya support Web site <http://www.avaya.com/support>.

 **Note:**

Before installing a Modular Messaging system, update the System Platform with the latest approved patches and service packs. Ensure that these patches and service packs are verified for use with Modular Messaging. You can download the latest patches and Service Packs from the Avaya support Web site (<http://www.avaya.com/support>). For more information on downloading and installing patches and Service Packs, see the *Administering Avaya Aura® System Platform* guide.

The System Platform installation has many parts to it.

It requires:

- Installing the server hardware.
- Connecting the server to the customer's network.
- Installing the System Platform software on the server.
- Configuring the Secure Access Link (SAL) gateway included in System Platform for remote support and alarming.

For more information about installing System Platform, see the *Installing and Configuring Avaya Aura® System Platform* guide available on the Avaya support Web site (<http://www.avaya.com/support>).

Configure SAL

SAL provides remote access, and alarming for serviceability of templates on System Platform, to Avaya service technicians and/or Avaya Partners. The high level steps for configuring SAL are as follows:

- Register the system: Registration must be initiated first to obtain the information that must be entered through the SAL administrative interface. To provide service and support to registered customers, Avaya assigns a Solution Element ID and Product ID to each SAL Gateway that is registered. This data is critical for the correct execution of various Avaya business functions and tools. For more information, see [Registering the system](#) on page 29
- Configure the SAL Gateway: The SAL Gateway provides remote access to those devices that are configured for remote access within it. It controls connections to managed elements, new or updated models, and verifies certificates for authentication. For more information, see [Configuring the SAL Gateway](#)

Configure the network settings

System Platform creates an internal, private bridge that allows virtual machines to communicate with each other. This private bridge does not have any connection to your LAN.

During installation, System Platform runs an algorithm to find a set of IP addresses that do not conflict with the addresses configured on the System Domain Network Configuration screen (during System Platform installation). However, it is still possible that the addresses selected may conflict with other addresses in your network. This address conflict could result in the failure of System Platform or an installed template to route packets correctly.

 **Note:**

To avoid such failures, before installing a template, check the Network Configuration page on the System Platform Web Console (**Server Management > Network Configuration**) to view the addresses allocated on the bridge named “avprivate”. If required, change the IP addresses for the “avprivate”.

For more information, see the *Administering Avaya Aura® System Platform* guide.

Date and time configuration

The date and time of your system are set during the System Platform installation. However, if you are installing a Modular Messaging system that uses a corporate Windows domain, you must verify that corporate domain time zone and the System Platform time zone are the same.

You can set the date and time from the System Platform Web Console (**Server Management > Date/Time Configuration**).

For more information, see the *Administering Avaya Aura® System Platform* guide.

Configure PBX

You must configure the PBX service settings for the Modular Messaging system using the appropriate configuration notes for the type of PBX or switch integration you use.

You can obtain the configuration notes required to integrate the MAS with the PBX at this site from the Avaya Support Web site: <http://www.avaya.com/support>.

Preparing for installation

You can install Modular Messaging from one of the following locations. Careful consideration should be given to which will work best in a specific customer scenario. If in doubt, and an avaya-certified business partner or Avaya technician is assisting with this installation, then ask for further guidance. Before starting the installation, you must set up the installation source.

 **Note:**

Modular Messaging does not support installation of the template using the SP CD/DVD and the Local File System option.

Installation location	Pre-installation setup	Notes
Recommended installation sources		
PLDS	You must register for the PLDS (https://plds.avaya.com) Web site. For more information, see Registering for PLDS on page 24.	The transfer from PLDS can be slow depending on your link speed.
SP Server	You must copy the template files from the optical media to the System Platform server. For more information, see Copying template from optical media to the System Platform server on page 24.	This method involves local resource commitments while copying files from the optical media to the System Platform server.
Alternative installation sources For more information, see <i>Appendix C: Alternative methods for preparing the installation source</i> .		
HTTP	You must copy the template files to an HTTP server that is accessible from the System Platform server. For more information, see Setting up the HTTP server on page 119.	This is the preferred method if more than one system needs to be installed, as the template files can be easily shared.
SP USB Disk	You must copy the template files from the optical media to a USB flash drive. For more information, see Setting up a USB flash drive on page 120.	This is the fastest method. However, the USB image may not be readily available during disaster recovery. Moreover, it requires a Linux machine to create the USB image.

Registering for PLDS

To register for the PLDS Web site:

Procedure

1. Go to the PLDS Web site (<https://plds.avaya.com>).
You will be redirected to the SSO Web site.
2. Log in to SSO using SSO ID and Password.
You will be redirected to the PLDS registration page.
3. If you are registering as a Avaya Partner, enter the Partner Link ID.
If you do not know your Link ID, send an e-mail to pradmin@avaya.com.
4. If you are registering as an customer, enter one of the following:
 - Company Sold-To
 - Ship-To number
 - License Authorization Code (LAC)
5. Click **Submit**.
Avaya will send you the PLDS access confirmation within one business day.

Copying template from optical media to the System Platform server

Perform the following tasks to copy the Modular Messaging template from optical media to the System Platform server.

Before you begin

You must have

- installed System Platform.
- the Modular Messaging template on the optical media. For more information, see [Obtain a Modular Messaging template](#) on page 20.

 **Note:**

If you have downloaded the Modular Messaging template from PLDS, you need to have them on optical media before copying the template to the System Platform server.

Procedure

1. Connect to dom0 of the System Platform. For more information, see [Accessing the System Domain \(Dom0\)](#) on page 33.
2. Insert the template CD into the CD-ROM of the System Platform.
 - If you are installing Modular Messaging without Web Client, insert **Modular Messaging single server configuration Template MAS/MSS**
 - If you are installing Modular Messaging with Web Client, insert **Modular Messaging single server configuration Template MAS/MSS/Web Client/WSO**
3. Type the following to mount the CD-ROM on the server:


```
mount -r -t iso9660 /dev/cdrom /mnt
```
4. Type the following to run the `setup_install_data.sh` script:


```
/mnt/setup_install_data.sh
```
5. Follow the on screen instructions and insert other two disks (**Modular Messaging single server configuration Application - DVD 1 of 2** and **Modular Messaging single server configuration Application - DVD 2 of 2**) when the system prompts you to.

Corporate Windows domain requirements

Note:

If you are setting up the Modular Messaging to use the private Windows domain, you can skip these requirements.

Before installing a Modular Messaging system that uses a corporate Windows domain, the administrator of the corporate Windows domain must create the user and computer accounts in the corporate Windows domain.

Creating user accounts in the corporate Windows domain

The administrator of the corporate Windows domain creates the technical support account, which is the user account name used for remote access, and the customer administration account in the corporate Windows domain.

About this task

 **Note:**

The corporate Windows domain administrator must log in to the Active Directory server using a logon that has privileges to add a user account to the corporate Windows domain.

Procedure

1. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
The system opens the **Active Directory Users and Computers** window.
2. Expand the directory for the corporate Windows domain.
3. Right-click **Users** and from the pop-up menu, select **New > User**.
4. In the **New Object** window, type the user account name, such as *techacct* or *custacct*, in both the Full Name and the User logon name fields.
5. Click **Next**.
6. Type the user account password in both the **Password** and **Confirm Password** fields.
7. Select the **Password never expires** check box.

 **Note:**

If you need to change the password for a Modular Messaging customer account, contact technical support for the procedure to change the password.

8. Click **Next**.
 9. Click **Finish**.
 10. Repeat this process as needed to make sure you create both technical support and the customer administration support accounts.
-

Creating computer accounts in the corporate Windows domain

The corporate Windows domain administrator creates computer accounts in the corporate Windows domain for all servers in the Voice Mail Domain (VMD). This includes the MSS, MAS, and, Web Client.

About this task

 **Note:**

The corporate Windows domain administrator must logon to the Active Directory server using a logon that has privileges to add a user account to the corporate Windows domain.

Procedure

1. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
The system opens **Active Directory Users and Computers** dialog box.
 2. Expand the directory for the corporate Windows domain.
 3. Right-click **Computers** and from the pop-up menu, select **New > Computer**.
 4. In the New Object window, in the **Computer Name** field, type the server name you want to create, such as *mymss* or *mymas*.
 5. Click **Change**. This specifies that a different user or group can add this computer to the corporate Windows domain.
 6. In the Select User or Group window, enter the customer administration account, such as *custacct*, that you created previously; see [Creating user accounts in the corporate Windows domain](#) on page 25.
 7. Click **Check Names**.
 8. Click **OK**.
 9. Click **Next**.
 10. Make sure that **This is a managed computer** check box is NOT selected.
 11. Click **Next**.
 12. Click **Finish**.
-

Chapter 3: Configuring the SAL Gateway and System Registration

Registering the system

Registering the System Platform and the Modular Messaging system will ensure that Avaya has a record of the system and it is ready for remote support delivery in the event it is needed. To provide service and support to registered customers, Avaya assigns a *Solution Element ID* (SE ID) and *Product ID*. This data is critical for the correct execution of various Avaya business functions and tools.

Procedure

To register the system, download and follow the instructions in the *Universal Install Product Registration Request Form*. This form is available on the Avaya Support Web site: <http://www.avaya.com/support> > More Resources > More > Additional Information > Avaya Partner Equipment Registration > Non-Regional Specific Documentation. You need to provide the following:

- a. Customer name
- b. Avaya Sold-to Number (customer number)
- c. Contact information to help Avaya contact you if there are questions

See *Table 8: Product registration information* on the [Planning form for installing Modular Messaging](#) on page 109.

Avaya uses this information to register your gateway. When the registration is complete, Avaya sends you:

- An e-mail with 5 sets of Solution Element ID and Product ID numbers. You will need these ID numbers to add managed devices to the SAL Gateway
- A list of the devices currently registered at this location
- A listing of your company locations.

Adding managed devices to the SAL Gateway

Before you begin

You must have:

- Installed the SAL Gateway
- An authorized user ID for the user to log in to the SAL Gateway
- 5 sets of Solution Element ID and Product ID numbers received from Avaya registration team.

About this task



Note:

You must add the SAL Gateway as the first device.

Procedure

1. Log on to the System Platform Web Console. For more information, see [Accessing the Console Domain \(CDOM\)](#) on page 34.
2. Click **Server Management > SAL Gateway Management**.
3. On the SAL Gateway Management page, click the **Launch SAL Gateway Management Portal** link.
4. On the SAL Gateway page, enter the authorized user ID and password to log in.
5. Click **Managed Element** on the navigation pane.
The system displays the Managed Element page.

On the Managed Element page, the system displays the following buttons: **Delete**, **Export managed elements**, **Add new**, and **Print**.

You need to add five new Managed Elements to the Managed Elements list specifically for the Single Server system being installed. These elements relate to the Solution Elements in the *Universal Install Product Registration Request Form* supplied by Avaya and needs to be entered as the Model in the Managed Element form.

Repeat steps 6 through 16 for each item in this table below:

Product	Element	Managed Element Model
SP (Dom0)	VSPU	VSP_1.0
SP (CDOM)	VSPU	VSPU_1.0
SAL	VSALGW	SAL_Gateway_1.0

Product	Element	Managed Element Model
MSS	VMSSR	MM_Storage_Server_1.0
MAS	VMAS	MM_Application_Server_1.0

6. Click **Add new**.
The system displays the Managed Element Configuration page.
7. In the **Host Name** field, enter a host name for the managed device. See *Table 8: Product registration information* on the [Planning form for installing Modular Messaging](#) on page 109.
8. In the **IP Address** field, enter the IP address of the managed device. See *Table 8: Product registration information* on the [Planning form for installing Modular Messaging](#) on page 109.
9. Select the **NIU** check box if you want to use a Network Interface Unit (NIU) port for remote access and select a value from the list box. The range of values allowed is 1-9.
10. Enter one of the elements from the list above in the **Model** field.
11. In the **Solution Element ID** field, enter the Solution Element ID of the device that is associated with this element as per the table above. For more information, see [Registering the system](#) on page 29.
The SAL Gateway uses the *Solution Element ID* value to uniquely identify the managed device.
12. In the **Product ID** field, enter the Product ID that is associated with this element as per the table above. For more information, see [Registering the system](#) on page 29.
SAL Gateway uses the *Product ID* value to uniquely identify the managed device associated with alarms originating from that device.
13. Select the **Provide Remote Access to this device** check box, if you want to allow the ability to remotely connect to the managed device.
This manages Remote Access On/Off status.
14. Select the **Transport alarms from this device** check box, if you want alarms from this device to be sent to the *Secure Access Concentrator Core Server*. This manages Alarming On/Off status.
15. Leave the **Collect Inventory for this device** check box cleared.
This feature is not available as yet.
16. Click **Add**.

Result

For more information, see *Secure Access Link 1.5 SAL Gateway Implementation Guide*.

Chapter 4: Accessing the System

Accessing the System

Accessing different parts of the system is achieved in different ways and can differ slightly depending on whether you are local to the system or remote. If you are not on the same network as the System Platform, you must use SAL to make a connection before using any of the access methods listed below.

The typical methods for accessing the different parts of the system are as follows:

- [Accessing the System Domain \(Dom0\)](#) on page 33
- [Accessing the Console Domain \(CDOM\)](#) on page 34
- [Accessing the MSS using the MSS Web console](#) on page 35
- [Accessing the MAS using RDC](#) on page 35
- [Accessing the Web Client server using RDC](#) on page 36

When the typical method of accessing the system is not available, perhaps due to network issues or installation issues, alternative methods are available in *Appendix D* as follows:

- [Accessing the MAS using the VNC viewer installed on the System Platform](#) on page 123
- [Accessing the MAS using the VNC viewer from a remote computer](#) on page 123
- [Accessing the MSS using PuTTY](#) on page 124
- [Accessing the MSS using virsh console command through PuTTY](#) on page 125

Accessing the System Domain (Dom0)

You need to access the System Domain (Dom0) primarily to copy the optical media to the System Platform server during installation. If you have physical access to the system, you can log on directly at the console using the root account. Alternatively, you need to set up a remote connection from your desktop using SSH (Secure Shell) Client such as PuTTY. After logging on, the system prompts you with the Linux command prompt.

About this task

To access the system using PuTTY:

Procedure

1. Start a PuTTY session from your desktop computer.
 2. Ensure that the connection type is set to SSH.
 3. Select **Connection > SSH > Tunnels**.
 4. In **Source port** field, enter the port number, for example, 5900
 5. In **Destination** field, enter the following:
`localhost:<VNC_PORT_NUMBER_OF_VM>`. To find out the VNC port number of the virtual machine, connect to the System Platform Web Console.
 - Open the System Platform Web Console (*http://ipaddress/webconsole*). Navigate to **Virtual Machine Management > Manage > Virtual Machine List** to find the VNC port
 - In the command prompt, run the following command: `virsh vncdisplay vm_hostname`, where `vm_hostname` is host name of the virtual machine
 6. Click **Add**.
 7. Select **Session > Host Name**, enter the **IP address** of Dom0.
 8. Type the following command after successful login: `su root`
 9. Enter the password for the `root` user.
-

Accessing the Console Domain (CDOM)

The Console Domain provides a graphical interface known as the System Platform Web Console for management of the system and administration of SAL and WebLM. You can access the Console Domain through a Web browser such as Internet Explorer or Mozilla Firefox from your desktop computer.

Procedure

1. Use your Web browser to navigate to the following URL: `http://<ipaddress>/webconsole`, where the IP Address is that of the Console Domain.

 **Important:**

The URL for the System Platform Web Console is case-sensitive.

2. On the System Platform Web Console, enter the user ID as *admin*.

3. Click **Continue**.
 4. Enter the password in the **Password** field.
 5. Click **Log On**.
-

Accessing the MSS using the MSS Web console

You need to access the MSS to administer subscribers, perform backups, and to administer other message store features using Web Administration screens. To access the MSS, use the Web Browser from your desktop computer:

Procedure

1. Use your Web browser to navigate to the following URL: `http://<mss-ipaddress>`.
The system opens the MSS Admin page.
 2. Enter the login name in the **Login** field.
 3. Enter the password in the **Password** field.
-

Accessing the MAS using RDC

You need to access the MAS to complete some of the installation steps, perform system administration and basic reporting, and to carry out maintenance activities. You can access the MAS through the Remote Desktop client from your computer.

Procedure

1. Click **Start > Run** to open the Run window.
2. In the **Open** field, type the following and press **Enter**:
 - If you are using Windows XP SP2 and below, type `mstsc /console`
 - If you are using Windows XP SP3 and above, type `mstsc /admin`The system opens the Remote Desktop Connection windows.
3. In the **Login** field, type the **IP address** of the MAS.

4. Click **Login**.
 5. Type the **User ID** and **Password**, enter the user ID for the customer account.
-

Accessing the Web Client server using RDC

You need to access the Web Client to complete some of the installation steps, and to carry out maintenance activities. You can access the Web Client through the Remote Desktop client from your computer.

Procedure

1. Click **Start > Run** to open the Run window.
 2. In the **Open** field, type the following and press **Enter**:
 - If you are using Windows XP SP2 and below, type `mstsc /console`
 - If you are using Windows XP SP3 and above, type `mstsc /admin`The system opens the Remote Desktop Connection windows.
 3. In the **Login** field, type the **IP address** of the Web Client.
 4. Click **Login**.
 5. Type the **User ID** and **Password**, enter the user ID for the customer account.
-

Chapter 5: Installing Avaya Modular Messaging

Overview

This chapter describes the steps to install Modular Messaging. After installing System Platform you can:

- Install Modular Messaging to run on System Platform.
- Verify and re-configure the parameters, using the System Platform pre-installation Web page.
- Manage the templates from the System Platform Web Console.

With the single server configuration, you can install Modular Messaging remotely. Single server configuration uses SAL Gateway to provide remote access. To install Modular Messaging remotely, you must have configured and registered SAL Gateway on the System Platform, before starting the installation.

- For more information on accessing the System Platform, see [How to access the System Platform](#).
- For more information on configuring the SAL Gateway, see [Configuring the SAL Gateway](#).

Before installing a Modular Messaging system:

- Before installing a Modular Messaging system, update the System Platform with the latest approved patches and service packs. Ensure that these patches and service packs are verified for use with Modular Messaging. You can download the latest patches and Service Packs from the Avaya support Web site (<http://www.avaya.com/support>). For more information on downloading and installing patches and Service Packs, see the *Administering Avaya Aura® System Platform* guide.
- Print the [Planning form for installing Modular Messaging](#) on page 109 and enter all data in the planning form, before you start installing Modular Messaging.
- Read Chapter 2: Installation prerequisites. This chapter describes installation requirements including where to find required documentation.
- Print the [Installation checklist](#) on page 14 and ensure that you follow the procedures in the same sequence as given in the checklist.

- Configure the SAL Gateway to get the remote access. For more information, see [Configuring the SAL Gateway](#).
- You must enable pop-ups in your Web browser. For more information on enabling pop-ups, see the online help of your browser.

Locating templates

 **Note:**

Modular Messaging does not support installation of the template using the SP CD/DVD and the Local File System option.

Before you begin

You must have set up the installation source. For more information, see [Preparing for installation](#) on page 23.

Procedure

1. Log in to the System Platform Web Console. For more information, see [How to access the System Platform](#).
2. Click the **Virtual Machine Management** tab.
3. Click **Solution Template**.
The system displays the Search Local and Remote Template page. Use this page to select a location from where you want to download the template.
4. Select one of the following locations from the list in the **Install Templates From** box:
 - PLDS
 - HTTP
 - SP Server
 - SP USB Disk
5. Click **Search** to display a list of template descriptor files (each available template has exactly one template descriptor file).
The system displays the Select Template page.

Next steps

Selecting the Modular Messaging template.

Selecting the Modular Messaging template

Caution:

Once you have opted for **Modular_messaging.ovf** template, you cannot add Web Client after the installation. Similarly, you cannot remove Web Client if you have opted for **wcwsso_mm.ovf** template. In both of these scenarios, you will have to reinstall the whole Modular Messaging system if you wish to add or remove Web Client after the template is installed.

Procedure

1. From the **Select Template** list, select the template that you want to install. System displays one of the following templates, depending on the product that you purchased:
 - **modular_messaging.ovf**: Modular Messaging without Web Client.
 - **wcwsso_mm.ovf**: Modular Messaging with Web Client.
2. Click **Select**.

Next steps

Customizing the template.

Customizing the template

You can choose to continue the installation with or without an EPW file. For an installation with the EPW file, the configurations parameters are pre-configured. However, you can verify and change the configuration parameters, if required. You must make a backup copy of the EPW file and store it in a safe location.

Procedure

1. Do one of the following:
 - If you do not have an existing EPW file, click **Continue without EPW file**. The system displays the Template Details page with information on the selected template and its Virtual Appliances. Continue with step 3.
 - If you have an existing EPW file, click **Continue with EPW file** and continue with step 2.
2. If you have an existing EPW file, perform the following steps to upload the EPW file:

 **Note:**

You can upload a ZIP (Legacy Zip 2.0 format) file only. Ensure that you have the Zipped EPW file ready and accessible, before you perform this step.

- a. In the Browse window, navigate and select the EPW file.
- b. Click **Open**.
- c. Click **Upload**.

The system displays the Template Details page with information on the selected template and its Virtual Appliances.

3. On the Template Details page, click **Install**.
The Template Installation page displays the progress of the template installation.
The system launches the Pre-installation Web page.

Next steps

Configuring the Modular Messaging template.

Configuring the Modular Messaging template

If you used the EPW file, the system pre-populates the fields in the Pre-installation Web page. You can verify and modify the details as appropriate.

If you did not use the EPW file, then enter the following Modular Messaging configuration details in the Pre-installation Web page.

Use the values from the planning form ([Planning form for installing Modular Messaging](#) on page 109) for configuring Modular Messaging.

 **Note:**

You must configure each configuration category before you install Modular Messaging. For detailed field descriptions, see *Appendix B: Field descriptions of planning form for installing Modular Messaging*.

Procedure

1. [Setting up the network](#) on page 41.
2. [Setting up the Modular Messaging network](#) on page 41.
3. [Setting up the Windows domain configuration](#) on page 42.
4. [Configuring Modular Messaging](#) on page 43.

5. [Creating Modular Messaging accounts](#) on page 43.
 6. [Configuring the switch integration](#) on page 44.
-

Setting up the network

You must specify information about the corporate network to allow Modular Messaging to route traffic through the corporate LAN and resolve computer names to IP addresses.

Procedure

1. Click **Networking**.
2. Click **Corporate Network Detail**.
3. On the Corporate Network Detail page, enter the details in the given fields. See *Table 1: Corporate Network Details / Domain Name Servers* on the [Planning form for installing Modular Messaging](#) on page 109.
4. Click **Domain Name Servers**.
5. On the Domain Name Servers page, enter the details in the given fields. See *Table 1: Corporate Network Details / Domain Name Servers* on the [Planning form for installing Modular Messaging](#) on page 109.

Next steps

Setting up the Modular Messaging network.

Related topics:

[Corporate Network Details field descriptions](#) on page 113

[Domain Name Servers field descriptions](#) on page 113

Setting up the Modular Messaging network

You must configure the Modular Messaging network to identify the Message Store Server (MSS) and Messaging Application Server (MAS) to the corporate network. Provide the IP addresses and Fully Qualified Domain Names (FQDNs) for each server. Ensure that you use only valid TCP/IP addresses.

Procedure

1. Click **Modular Messaging Networking**.
2. On the Corporate MM Networking Details page, enter the details in the given fields. See *Table 2: Corporate Modular Messaging details* on the [Planning form for installing Modular Messaging](#) on page 109.

Next steps

Setting up the Windows domain configuration.

Related topics:

[Corporate MM networking field descriptions](#) on page 114

Setting up the Windows domain configuration

You must specify the details of the corporate Windows domain to which you want to add the Modular Messaging system to join.

Procedure

1. Click **Windows Domain Configuration**.
2. Select the option to join either a corporate domain or a private domain.
3. To join the private domain, enter the name of the Windows domain.
4. To join the corporate domain:
 - a. Enter the host name of the domain controller.
 - b. Enter the name of the corporate Windows domain.

See *Table 3: Windows domain configuration* on the [Planning form for installing Modular Messaging](#) on page 109.

Next steps

Configuring Modular Messaging.

Related topics:

[Windows Domain field descriptions](#) on page 115

Configuring Modular Messaging

You must enter the parameters for configuring Modular Messaging. You can select the languages used for Telephone User Interface (TUI) announcements and Text-to-Speech conversion.

About this task

**Note:**

The system displays the Web Client configuration fields, only if you have selected the Modular Messaging with Web Client template (*wcwsso_mm.ovf*).

Procedure

1. Click **Modular Messaging Configuration**.
2. On the Modular Messaging Configuration page, enter the details in the given fields. See *Table 4: Modular Messaging configuration* on the [Planning form for installing Modular Messaging](#) on page 109.
3. To configure Modular Messaging Web Client, you must enter the IP address and host name of the Web Client server. You must also enter the windows license key for the Web Client server.

Next steps

Creating local administrator accounts.

Related topics:

[Modular Messaging Configuration field descriptions](#) on page 115

Creating Modular Messaging accounts

You must configure and set up the Modular Messaging accounts.

Procedure

1. Click **Modular Messaging Accounts**.
2. On the MSS Account Information page, enter the details in the given fields. See *Table 5: Modular Messaging accounts - MSS account info* on the [Planning form for installing Modular Messaging](#) on page 109.

The MSS is configured to allow access only by those computers that are identified as trusted servers. Trusted servers are clients that have permission to read data from and write data to the LDAP directory on the MSS.

3. Click **MAS Logon Accounts and Password**.
4. On the MAS Logon Accounts and Password page, enter the details in the given fields. See *Table 6: Modular Messaging accounts - MAS login accounts & passwords* on the [Planning form for installing Modular Messaging](#) on page 109. Remote support personnel use the technical support account to access the system and provide technical support. The customer account is used by customers to monitor the system.
5. Click **MAS Admin Account**.
6. On the MAS Admin Account page, enter the details in the given fields. See *Table 6: Modular Messaging accounts - MAS login accounts & passwords* on the [Planning form for installing Modular Messaging](#) on page 109. Specify the name and password of the local administrator account for MAS.

Next steps

Setting up the switch integration.

Related topics:

[Modular Messaging Accounts field descriptions](#) on page 116

Configuring the switch integration

You must configure switch integration for the Modular Messaging. Switch integration (SWIN) provides connectivity between the Private Branch Exchange (PBX) and the Messaging Application Server (MAS).

Note:

Single server configuration supports only SIP-based switch integrations.

Procedure

1. Click **PBX Integration**.
2. On the Switch Integration Information page, enter the details in the given fields. See *Table 7: Switch integration information* on the [Planning form for installing Modular Messaging](#) on page 109. For more information, see *PBX Configuration* in the *Modular Messaging with Avaya MSS - MAS Administration Guide*.

Next steps

Saving the configuration.

Related topics:

[Switch Integration Information field descriptions](#) on page 118

Saving the configuration

You must save your configuration parameters for installing Avaya Modular Messaging on the System Platform.

! **Important:**

The system enables the **Save & Continue** button only if you have entered all the details correctly.

Procedure

1. Click **Save & Continue**. The system displays the Finish page.
2. Click **Click here to download EPW file** to save the EPW file.

! **Important:**

You must save the EPW file for later use. This EPW file will be required for disaster recovery.

3. On the Finish page, you can view the configuration details that you specified.

***** **Note:**

If the system encounters any error in the configuration, the system displays the error in red on the Finish page. Make corrections to the problem field and return to the Finish page to continue with the installation.

4. Click **Install** to continue with the installation.

Result

The pre-installation Web page closes and you can see the template installation progress window. The entire installation process takes about 60 to 90 minutes.

***** **Note:**

Do not attempt to configure the virtual machines while the post installation process is in progress. All the applications are configured at this stage. Attempting to configure the system too early may result in your changes being lost or the installation being blocked from completing its tasks.

If there is any error during the process, the system displays the error on screen in bold letters together with a warning symbol in the extreme right column in the screen. Investigate such a message immediately.

Verifying the installation

About this task

After completing the installation, verify that the Modular Messaging components are running. You can do this by checking the Manage page on System Platform Web Console.

Procedure

1. Click **Virtual Machine Management > Manage**.
The system displays the Virtual Machine List page.
2. Verify the following:
 - **Name:** Name of the virtual machines running on System Platform.
 - **Version:** Version number of the respective virtual machine.
 - **IP Address:** IP address of the virtual machine.
 - **Maximum Memory:** This is a display only field. The value is set by Avaya, and cannot be configured by the users. The amount of physical memory from the total server memory the virtual machine has allocated in the template file.
 - **Maximum Virtual CPUs:** This is a display only field. The value is set by the Avaya services team, and cannot be configured by the users. CPU allocation for the virtual machine from the template file.
 - **CPU Time:** The amount of CPU time the virtual machine has had since the last reboot and this is not the same as up time. This field is set by the Avaya services team to investigate issues around machine processor occupancy.
 - **State:** Current status of the virtual machine.
 - **Application State:** Current status of the application (respective virtual machine).

Next steps

After completing the installation, you must configure the newly installed virtual machines (MAS, MSS, and Web Client if installed). For more information on configuration, see *Chapter 6: Configuring Modular Messaging*.

If the installation is not successful, check the troubleshooting steps. For more information on troubleshooting, see *Chapter 13: Troubleshooting*.

Chapter 6: Configuring Modular Messaging

Overview

This chapter describes the step to configure Modular Messaging on a single server configuration.

Adding the MSS as a trusted site

Increased security on the Avaya MAS requires you to set up the MSS as a trusted site if you access the MSS from the MAS. You must do this task the first time you try to access the MSS from the MAS.

Procedure

1. On the MAS, open Internet Explorer.
2. If the system displays a warning that the Internet Explorer Enhanced Security Configuration is enabled, click **OK**.
3. In the Internet Explorer main window, select **Tools > Internet Options**.
4. In the Internet Options window, click the **Security** tab.
5. Click **Trusted Sites** so the item is highlighted, and then click the **Sites** button.
6. In the Trusted sites window:
 - a. Verify that the **Require server verification (https:) for all sites in this zone** check box is cleared.
 - b. Under **Add this Web site to the zone**, type the full corporate computer name of the MSS and click **Add**.



Tip:

Do not enter http:// or https://, or the browser might not find the server automatically.

- c. Click **OK** to close the Trusted sites window.
 7. Click **OK** to close the Internet Options window.
-

Preparing the MAS

Activating Microsoft Windows

You must activate the Microsoft Windows operating system. The Microsoft Windows activation procedure requires you to use either the Internet or a telephone. Use the method that is most appropriate for the site.

Activating Microsoft Windows using the Internet

Procedure

1. Double-click the Internet Explorer icon on the desktop.
2. Click **OK** at the Enhanced Security message.
3. In the Internet Explorer window, click **Tools > Internet Options**.
4. In the Internet Options window, click the **Connections** tab.
 - a. Click **LAN Settings**.
 - b. In the Local Area Connection (LAN) Settings window, specify the settings to use for this site.
 - c. Click **OK** to close the Local Area Connection (LAN) Settings window.
5. Click **OK** to close the Internet Options window.
6. Close the Internet Explorer.
7. Click **Start > Activate Windows**.
8. In the Activate Windows window:
 - a. Click **Yes, let's activate Windows over the Internet now**.
 - b. Click **Next**.

The program checks for Internet connectivity. If connectivity fails, you can set up or modify the Internet connectivity settings. Complete the screen and click **Next** to continue.

9. On the Thank you screen, click **OK**.
-

Activating Microsoft Windows using a telephone

To activate the Microsoft Windows operating system using a telephone:

Procedure

1. Click **Start > Activate Windows**.
 2. In the Activate Windows window:
 - a. Click **Yes, I want to telephone a customer service representative to activate Windows**.
 - b. Click **Next**.
 3. On the Activate Windows by phone screen:
 - a. Select the country where you installed the Modular Messaging system.
 - b. Call the appropriate telephone number shown on the screen.
 - c. Follow the voice prompts or the directions from the customer service representative to get the unique installation ID shown on the screen.
 - d. Enter the confirmation ID that the automated system or the customer service representative gives you.
 - e. Click **Next**.
 4. On the Confirmation screen, click **Finish**.
-

Updating Microsoft Windows

After installation, you must install the latest updates for Microsoft Windows, including operating system updates and security patches. These software updates protect the system from known security weaknesses. Check with the appropriate Windows administrator for the software update procedures to use at this site.

Installing and administering anti-virus software

About this task

Avaya recommends that you install anti-virus software on any Microsoft Windows computer that runs Avaya Modular Messaging software. The anti-virus software used and the method of installation depends on site specific requirements.

 **Note:**

If you cannot install the required files using the customer account login, log off and then log in using the local administration account name.

Procedure

1. Install the anti-virus software using the installation method that is appropriate for this site.
 2. Configure the anti-virus software to work correctly with Avaya Modular Messaging software.
-

Configuring licenses

License management

After installing Modular Messaging, you must install the license. Avaya provides the licenses through the PLDS (<https://plds.avaya.com>). After downloading the licenses from the PLDS, you must install them on the System Platform WebLM server.

For more information on managing licenses, see *Getting Started with Avaya PLDS* guide available on the Avaya Support Web site at <http://www.avaya.com/support>.

The following three WebLM configurations are possible:

- WebLM server on the System Platform: A WebLM server is installed as part of the System Platform installation. You must generate the Avaya WebLM license using the virtual MAC

address of the System Platform Console Domain (CDOM). This is a system generated MAC address and NOT the same as the real MAC address of eth0.

- Existing WebLM server: If you already have a WebLM server that you are using for licensing other Avaya products.
- WebLM server on a standalone server: If you choose to install the WebLM on a standalone server, follow the instructions provided in *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at <http://www.avaya.com/support>.

For more information on WebLM configurations, see *Avaya Modular Messaging Concepts and Planning Guide*.

Obtaining licenses

About this task

Obtain a new license file from Product Licensing and Delivery System (PLDS) to be applied on a Web License Manager (WebLM) server. You can associate one license file with multiple Modular Messaging systems and therefore consideration must be given to how the licenses will be distributed. In most cases, these decisions are made before the license is obtained from PLDS. For more information on possible WebLM configurations, see *Licensing* in the *Avaya Modular Messaging Concepts and Planning Guide*.

Caution:

Do not change your license file after you receive it from Avaya. WebLM does not accept a modified license file.

Procedure

Use one of the following methods to obtain the license file:

- If you (or the registered owner of your site) receive a License Activation Code (LAC) e-mail from PLDS, use this LAC to obtain the Modular Messaging license from the PLDS Web site at <https://plds.avaya.com>.
- An Avaya Partner or an Avaya Associate who has permissions in PLDS for your site or sales order can access PLDS and generate a new license file for you. You must provide the MAC address of the WebLM server and the number of Modular Messaging subscribers, to generate the license file.

For more information about using PLDS, see *Getting Started with Avaya PLDS* guide available on the Avaya Support Web site at <http://www.avaya.com/support>.

Next steps

Applying license file on the WebLM server.

Applying license file on the WebLM server

Procedure

1. If you are applying the license file on:
 - a WebLM server that is installed with the System platform, use the System Platform Web Console to log on to the WebLM server.
 - an existing WebLM server or standalone server, in the Web browser, enter the URL for the WebLM server in the format, `https:// <ip-address>:<WebLM_Port>/WebLM/LicenseServer`.
2. On the WebLM License Manager page, follow the instructions to manage licenses.
For more information on managing licenses through Avaya WebLM, see *Installing and Configuring Avaya WebLM Server*.

Next steps

Importing certificates from license.

Importing certificates from license

About this task

You must import the license file using the Voice Mail System Configuration (VMSC) application to apply the certificates to your VMD.



Note:

To import the certificates, you must copy the license file to the MAS on which you use VMSC to import the certificates.

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
2. Click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**.
The Voice Mail System Configuration window opens.
3. Under the Voice Mail Domain (VMD), navigate to **Licensing**.
4. Right-click **Licensing** and select **Import Certificates from License**.
The system opens the **License Import Wizard**.

5. Complete the wizard.
6. Restart the Messaging Application Server service on the MAS.

Next steps

Verifying the WebLM URL in VMSC.

Verifying the WebLM URL in VMSC

Verify the URL for the WebLM server in VMSC on the MAS.

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
2. Click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**.
The Voice Mail System Configuration window opens.
3. Under the Voice Mail Domain (VMD), double-click **Licensing**.
The system displays the Licensing - Voice Mail Domain window.
4. On the **Licensing** tab, complete the following:
 - a. In the **WebLM URL** field, verify that the system displays the correct URL, if required modify the IP Address or fully qualified domain name for WebLM server. For example, *https://<FQDN of the WebLM server>:<Port Number>/WebLM/LicenseServer*.
 - b. Click **OK**.
5. Restart the Messaging Application Server service on the MAS.
6. On the **Licensing** tab, in the **License Mode** field, verify that the system displays the status as Normal.
7. On the WebLM server, verify the number of available subscriber licenses and TTS licenses.
8. Verify the product ID for the Modular Messaging.

Entering Product ID for the MAS

If Avaya is to support this system, you must enter the MAS product ID. For more information on system registration, see [Registering the system](#) on page 29.

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
 2. From the VMSC, double-click **Message Application Servers**.
 3. Double-click the MAS and select **Serviceability**.
 4. On the Serviceability window, type the product ID for the MAS in the **Product Identifier** field.
 5. Click **OK**.
-

Configure specific features on an MAS

Configuring specific features as needed

About this task

You need to configure features such as Call Me, MWI, Fax, and Offline message store after the installation. Use the procedures in this section to manually configure the other features and Multilingual TTS, if necessary.

Procedure

Configure the features that are required for this MAS:

- [Configuring Call Me service](#) on page 55
 - [Configuring Notify Me](#) on page 55
 - [Configuring MWI service](#) on page 55
 - [Configuring MM Audit Service](#) on page 56
 - [Configuring the MM Fax Sender server](#) on page 57
 - [Configuring languages and multi-lingual TTS](#) on page 61
 - [Configuring offline access to messages](#) on page 62
-

Configuring Call Me service

About this task

To configure the Call Me service for the VMD:

Procedure

1. In the Voice Mail System Configuration window, under the VMD, double-click **Call Me**.
 2. In the Call Me - Voice Mail Domain window, on the **General** tab, click the **Enable Call Me** check box.
 3. For **MAS Call Me Server**, specify the name of the MAS. If this field is blank:
 - a. Click ... next to the field.
 - b. In the **Select Computer** window, enter the name of the MAS.
 - c. Click **Check Names**.
 - d. Click **OK** to accept the MAS name and close the window.
 4. Click **OK** to close this window.
-

Configuring Notify Me

About this task

To configure the Notify Me for the VMD:

Procedure

1. In the Voice Mail System Configuration window, under the VMD, double-click **Notify Me**.
 2. On the **General** tab, select the **Enable Notify Me** check box.
 3. Click **OK**.
-

Configuring MWI service

About this task

To configure the Message Waiting Indicator (MWI) service for the VMD:

Procedure

1. In the Voice Mail System Configuration window, under the VMD, double-click **Message Waiting Indicator**.
 2. In the Message Waiting Indicator - Voice Mail Domain window, on the **General** tab, select the **Enable Message Waiting Indicator (MWI)** check box.
 3. For MAS MWI server, specify the name of the MAS. If this field is blank:
 - a. Click ... next to the field.
 - b. In the Select Computer window, enter the name of the MAS.
 - c. Click **Check Names**.
 - d. Click **OK** to accept the MAS name and close the window.
 4. For the **Limit requests** and **Maximum requests** per minute fields, use the values specified in the configuration notes for your PBX integration type.
 5. In the **Messaging Application Servers that support MWI** dialog box, add a server name:
 - a. Click the **Add** button at the top of the list box. The **Add** button looks like a dashed box.
 - b. The list box displays a data entry field and a ... button. Click the ... button.
 - c. In the Select Computer window, double-click the name of MAS.
 - d. Click **OK** to close the Select Computer window.
 6. Click **OK** to close this window.
-

Configuring MM Audit Service

About this task

To configure the MM Audit service for the VMD:

Procedure

1. In the Voice Mail System Configuration window, under the VMD, double-click **Auditing**.
2. On the **General** tab, select the **Enable Auditing** check box.
3. In the **Audit server** field, enter the name of the server, or use the browse button ... to select the name:
 - a. In the Select Computer window, enter the local host name of the MAS.
 - b. Click **Check Names**.

- c. Click **OK** to accept the MAS name and close the window.
4. In the **Audit event retention (days)** field, enter the number of days before events are purged from the audit database.
5. In the **Database server** field, enter the name of the server where the Audit database resides or use the browse button ... to select the server.
6. In the **Database name** field, enter the name of the Audit Server SQL database.
7. In the **Database instance** field, enter the name of the Audit Server SQLDatabase instance containing audit events.
8. Click **OK** to close this window.
Audit service can be configured to use the syslog protocol to allow third-party system administration tools to be used with Modular Messaging.

Configuring the MM Fax Sender server

Complete the following steps on the MAS.

About this task

To configure the MM Fax Sender server, complete the following steps:

Procedure

1. [Configuring the MM Fax Sender server in VMSC](#) on page 57.
2. [Configuring one-way trust in a private Windows domain](#) on page 58.
3. [Sharing the MM Fax Printer](#) on page 59.
4. [Assigning permissions to the Fax Service Manager](#) on page 60.
5. [Creating a dialing rule](#) on page 61.

Configuring the MM Fax Sender server in VMSC

To configure the MM Fax Sender server in VMSC, complete the following steps:

Procedure

1. In the **Voice Mail System Configuration** window, under VMD, double-click **Fax**.
2. In the Fax - Voice Mail Domain window, on the **General** tab:
 - a. Select the **Fax Enable** check box.
 - b. Next to **MM Fax Sender server**, click **Browse**.

- c. In the Select Computer window, enter the name of the MAS.
 - d. Click **Check Names**.
 - e. Click **OK** to accept the MAS name and close the window.
 - f. For **Fax Mailbox**, enter the mailbox number that is used for outgoing faxes on the MSS.
 - g. For **Company Fax Number**, enter the number of the customer's central fax machine.
3. Click the **Advanced** button.
 - a. In the Advanced Fax window, change the value of the **Fax Concurrent Outgoing Calls** to the customer-specified number.
 - b. Change other options if required.
 - c. Click **OK** to close the window.
 4. Click **OK** to close the Fax - Voice Mail Domain window.
The system displays a "restart" window.
 5. Click **OK**.
 6. In the Voice Mail System Configuration window, expand **Security**.
 7. Double-click **Messaging Servers Administration**.
 8. In the Message Servers - Voice Mail Domain window, on the **Message Servers** tab:
 - a. Note that the Credentials list shows entries for LDAP, IMAPI, and IMAP4.
 - b. Click the key button above the list to add a new entry for fax.
The system displays **FAX** in the box.
 - c. Click in the Password column next to the new Fax entry.
 - d. Type the password for the fax mailbox and press **Enter**. This value must be numeric and must be the same as has been set on the fax mailbox on the MSS.
 - e. Click **OK** to close this window.
-

Configuring one-way trust in a private Windows domain

To configure one-way trust between the private Windows domain and the customer's corporate Windows domain, complete the following steps:

About this task

 **Note:**

Use the following steps only for systems that run in the private Windows domain:

 **Important:**

When you configure the MM Fax Sender server, an account with the credentials to create a trust relationship between the private and corporate Windows domains must be available or a representative from customer's corporate IT group who has an account with the credentials is available. If the IT representative cannot provide the account information during installation, skip the MM Fax Sender server configuration and complete the rest of the Modular Messaging installation. Proceed with [Configuring the MM Fax Sender server](#) on page 57 and complete the configuration of the one-way trust when the account information is available.

Procedure

1. Log into the Active Directory server.
 2. Click **Start > Programs > Administrative Tools > Active Directory Domains and Trusts**.
 3. In the Active Directory Domains and Trusts window, right-click the private Windows domain and then click **Properties**.
 4. Click the **Trusts** tab.
 5. On the **Trusts** tab, click **New Trust** and then click **Next**.
 6. Enter the name of the corporate Windows domain you want the private Windows domain to trust and then click **Next**.
 7. Click **One-Way: Outgoing** and then click **Next**.
 8. Click **Both this Domain and the Specified Domain** and then click **Next**.
 9. The customer's corporate I/T person types the account name and password for an account in the corporate Windows domain that has privileges to create a trust relationship and then click **Next**.
 10. Click **Validate the Trust** and then click **Next**.
 11. Click **Finish**.
-

Sharing the MM Fax Printer

To share the MM Fax Printer, complete the following steps:

Procedure

1. Verify that Windows Fax Service is **Started** and set to **Automatic**.
2. Click **Start > Settings > Printers and Faxes**.
3. In the **Printers and Faxes** window, right-click the **Fax** and select **Properties**.
4. Click the **Security** tab.

5. Add the Network Service user and assign that user **Print, Manage Printers, and Manage Documents** permissions.
6. Click the **Sharing** tab.
7. Select the **Share this printer** check box. Leave the share name as **Fax**.
8. Select the **List in the directory** check box.
9. Click **Additional Drivers**. The system opens the **Additional Drivers** dialog box.
10. Select the client operating systems installed on the network that can use the Fax Printer. The Fax Printer drivers are downloaded when you first connect the system to the Fax Printer.
11. Click **OK**.
12. Click the **Security** tab.
13. Verify that **Everyone** is assigned Fax permissions on the share.

 **Note:**

If you want to limit the access to the Fax printer share, remove the Everyone group and add Fax permission to the Active Directory Users or Groups you want to provide access to print faxes using the MM Fax Printer.

Assigning permissions to the Fax Service Manager

To assign permissions to the Fax Service Manager, use the following steps:

Procedure

1. Click the **Configuration** tab.
2. Select **Fax Service Manager**.
3. Right-click **Fax (local)** and select **Properties**.
4. Click the **Security** tab.
5. Add the Network Service Account to the list of users and groups with access.
6. Assign **Fax, Manage Fax Configuration and Manage Fax Documents** permissions to the Network Service Account.
7. Assign **Everyone** the **Fax** permissions for the Fax Service Manager.

 **Note:**

If you want to limit the access to the Fax printer share, make the same permission changes to the Fax Service Manager as that of the Fax printer share.

8. Exit all windows.
-

Creating a dialing rule

To create a dialing rule for the Phone and Modem, complete the following:

Procedure

1. Click **Start > Settings > Control Panel > Phone and Modem Options**.
 2. If a dialing rule is not already created, click **New** in the Dialing Rules tab to create a dialing rule.
 3. Specify the location details and the dialing rules for the MAS.
 4. Click **OK** to save the dialing rule and close the New Location window.
 5. Click **OK**.
-

Configuring languages and multi-lingual TTS

About this task

Enable Multi-Lingual TTS only if it is required at the site. To configure multiple languages or Text-to-Speech (TTS) feature:

Procedure

1. In the Voice Mail System Configuration window, under the VMD, such as vmdom, double-click **Languages**.
 2. In the Languages - Voice Mail Domain window:
 - a. For **Primary Language**, select the primary announcement language (prompt set) that is to be used at this site.
 - b. If multi-lingual Text-to-Speech (TTS) is used at this site:
 - i. Select the **Enable Multilingual Text to Speech** check box.
 - ii. In the list box, select all the languages to be used for TTS at this site.
 3. Click **OK** to close this window.
-

Configuring offline access to messages

About this task

To configure offline access to subscriber messages:

Procedure

1. In the Voice Mail System Configuration window, under VMD, double-click **Messaging**.
 2. In the Messaging - Voice Mail Domain window, click the **Offline Access** tab.
 3. Select the **Enable offline access to messages** check box.
 4. Change any other parameters in this window as needed.
 5. Click **OK** to close the window.
 6. Restart the MAS service.
-

Chapter 7: Updating Modular Messaging

Overview

You must update the Avaya Modular Messaging software after an installation or upgrade to bring it up to date with the latest changes. Software updates might include the latest Avaya Service Pack or Avaya software patches.

Visit the Avaya Support site (<http://www.avaya.com/support>) and see the latest Release Notes to know about the latest patches, and access the regular updates and patches for the Modular Messaging provided by Avaya.

Downloading software updates

Get the latest Avaya software updates from the Web.

Procedure

1. Go to Avaya Support Web site at <http://www.avaya.com/support>.
2. Download the files needed to update the Modular Messaging system.
Ensure that you download both the software files and any instructions required to install the software updates.

Next steps

Copying software updates to the MAS.

Copying software updates to the MAS

You must copy the Avaya software updates to the MAS. You can copy the Avaya software updates to the MAS using the System Platform Web Console or using your Windows explorer. Complete the following steps to copy the software updates to the MAS using the System Platform Web Console.

Procedure

1. Log on to the System Platform Web Console.
2. Click **Server Management > Patch Management** from the System Platform Web Console.
3. Click **Download/Upload**.
4. On the Search Local and Remote Patch page, select one of the following locations to search for the software updates.
 - Select **HTTP** or **SP Server**, if you copied the software updates to one of these servers, and specify the **Patch URL**.
 - Select **Local File System**, if you copied the software updates to your computer, and then click **Browser** to locate the software updates on your computer and then upload.
5. Click **Search** to search for the required software updates.
6. Choose the software update and click **Select**.
7. Click **Manage**.
The Patch List page displays the list of software updates and the current status of the software updates.
8. On the Patch List page, click on a patch ID to see the details.
9. On the Patch Detail page, click **Install**.
The system copies the selected software update to the C:\MM_PATCH_FILES folder of the MAS.

 **Note:**

Even if you are using the Windows explorer to copy the software updates, ensure that you copy the files to C:\MM_PATCH_FILES folder on the MAS.

Next steps

Installing software updates on the MAS.

Installing software updates on the MAS

 **Important:**

Always read the Release notes for each software update which provide specific information about the software update. The following are general instructions for installing updates on an MAS.

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.

 **Note:**

If you are installing software updates using remote desktop you should connect to the console of the server you are installing the software updates on to.

2. Log on as a Domain Administrator.
 - In a private Windows domain, use the domain administrator account name, such as *dom-admin*.
 - In a corporate Windows domain, use the customer account name, such as *custacct*.
3. Double-click the software update file, such as *MAS520100.exe* from the `C:\MM_PATCH_FILES` folder of the MAS.
The program unpacks the contents of the file and runs the Modular Messaging Installation Wizard.
4. In the Modular Messaging Installation Wizard window, Click **Install**.

 **Note:**

If the Install button is not active, you do not need to apply these software updates to the system.

5. If you are installing a Service Pack, an Installation Wizard - Update Warning window opens. This window displays the patches and Service Packs that the program must remove before the update can continue. Click **Continue**.
6. After you click **Install**, monitor the software update progress:
 - a. In the Services window, the Modular Messaging Installation Wizard stops all appropriate Modular Messaging and related services.
 - b. Windows Installer then installs all relevant software updates on the MAS.
 - c. If any updates apply to the MSS, the program transfers the appropriate files to the MSS.
 - d. If prompted, reboot the MAS.

Next steps

Verifying software updates on the MAS.

Verifying software updates on the MAS

Procedure

1. To verify the software updates installed on the MAS:
 - a. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
 - b. Select **Start > Programs > Avaya Modular Messaging**.
 - c. Click the **About Modular Messaging** tab.
The About tab shows the version of MM installed
 - d. Click the **Patches** tab.
You can see the Service Packs and Patches installed on the system.
2. After installation and verification is complete, close all open windows.

Next steps

Installing software updates on the MSS.

Installing software updates on the MSS

Procedure

1. Connect to the MSS using MSS Web console. For more information, see [Accessing the MSS using the MSS Web console](#) on page 35.
2. From the Software Management menu, click **Software Update > Service Pack**.



Caution:

If you see a warning about the backup that is incomplete within the last 2 hours, click **Cancel**. Save the server data before you continue.

3. The system might report that the installed version is current. In this case, the MSS already has the most recent software updates installed. Do not take any further action.
4. If an update is present, click **Proceed with Service Pack Installation**.
The system reports that a reboot is required.
5. Click **Proceed with Installation**.
The system installs the updates on the MSS.

6. Verify that the installation completed successfully.
7. Click **Reboot servername**.
8. At the reboot warning message, click **OK** to continue.
The system displays status messages as the server shuts down the messaging software.

The shutdown process can take several minutes.

Next steps

Installing software updates on the Web Client server.

Installing software updates on the Web Client server

Procedure

1. Copy the software updates file from the `C:\MM_PATCH_FILES` folder of the MAS to the `C:\MM_PATCH_FILES` folder of the Web Client:
 - a. From the MAS, click **Start > Run** to open the Run window.
 - b. In the **Open** field, type the following and press **Enter**:
`<webclientIP>\C$\MM_PATCH_FILES`
 - c. Copy the software updates file to the `C:\MM_PATCH_FILES` folder of the Web Client
2. Log on to the Web Client server as a Domain Administrator.
 - In a private Windows domain, use the domain administrator account name, such as *dom-admin*.
 - In a corporate Windows domain, use the customer account name, such as *custacct*.
3. Double-click the software update file, such as *MAS520100.exe*, from the `C:\MM_PATCH_FILES` folder of the Web Client.
The program unpacks the file and then runs the Modular Messaging Installation Wizard.
4. In the Modular Messaging Installation Wizard window:
 - a. Select all applicable software updates for this system.
 - b. Click **Install**.

 **Note:**

If the Install button is not active, you do not need to apply these software updates to the system.

5. If you are installing a Service Pack, an Installation Wizard - Update Warning window opens. This window displays the patches and Service Packs that the program must remove before the update can continue. Click **Continue**.
 6. After you click **Install**, monitor the software update progress:
 - a. In the Services window, the Modular Messaging Installation Wizard stops all appropriate Modular Messaging and related services.
 - b. Windows Installer then installs all relevant software updates on the Web Client.
 - c. If any updates apply to the MSS, the program transfers the appropriate files to the MSS.
 - d. If prompted, reboot the Web Client.
-

Chapter 8: Performing acceptance tests for a new installation

Acceptance tests ensure that the Modular Messaging system works as expected.

 **Note:**

- You must first install software updates if any, before performing acceptance tests.
- You must wait for about 1 minute for MSS and MAS to synchronize their data after you add test subscribers. Otherwise, the acceptance tests do not run correctly.

Related topics:

[Adding test subscribers](#) on page 69

[Leaving a call answer message](#) on page 71

[Retrieving test messages in integrated mode](#) on page 72

[Creating and sending a test message in non-integrated mode](#) on page 74

[Testing the outcalling capability](#) on page 75

[Creating and printing a fax message](#) on page 77

Adding test subscribers

About this task

Set up at least one local subscriber to test the system. If you have to test multiple types of telephone user interface (TUI), set up a test subscriber for each TUI.

Procedure

1. Log on to the MSS Web Admin as `sa` using the appropriate password.
2. From the Manage Subscribers page, next to the **Local Subscriber Mailbox Number** field, click **Add or Edit**.
The system displays the Add Local Subscriber page.
3. Fill in the fields in the Subscriber Information section. Click **Help** if you need more information to complete any of the fields on this page.
4. Scroll down and click **Save**.

5. At the confirmation prompt, click **OK**.
6. If you want to test multiple user interfaces, repeat Steps 1 through 5 to set up an additional test subscriber, as required.

Example

Subscriber page sample settings:

Field	Setting
Last Name	Aria
First Name	Test
Password	1
Mailbox Number	Type a valid number for the test subscriber mailbox. Usually this is the same number as the primary telephone (PBX) extension for that subscriber. Enter 3 to 50 digits as required by the dial plan.
Class of Service	<p>Set up a unique class of service (COS) for each telephone user interface (TUI) that this Modular Messaging system supports. Activate the following features:</p> <ul style="list-style-type: none"> • Leave Message Waiting Indication Allowed set to yes. • Set all supported notification options to yes. For example, set Call Me, Find Me, and Notify Me to yes. • If fax service is required, set Outbound Fax Calls to yes. • Set Record Mailbox Greetings to yes. • To access the mailbox, set Restrict Client Access to no. Mailbox clients include the Microsoft Outlook client and the IBM Lotus Notes client. • For Telephone User Interface, select the interface required for this class of service. TUI interfaces include MM Aria, MM AUDIX, and MM Serenade.
Numeric Address	Type an address that is unique within the messaging network. The numeric address can include or be identical to the Mailbox Number . Enter 3-to-50 digits as required by the dial plan.

Related topics:

[Performing acceptance tests for a new installation](#) on page 69

[Leaving a call answer message](#) on page 71

[Retrieving test messages in integrated mode](#) on page 72

[Creating and sending a test message in non-integrated mode](#) on page 74

[Testing the outcalling capability](#) on page 75

[Creating and printing a fax message](#) on page 77

Running acceptance tests

Leaving a call answer message

The following test works only if call-coverage is assigned on the switch to route unanswered calls to the extension for the test subscriber.

Procedure

1. Call the first test subscriber extension from another telephone. Use an extension for which you have access to the physical telephone. Allow the Modular Messaging system to answer.
2. Speak into the telephone and record a test message after the tone, for example: This is a test call answer message.
3. Hang up the telephone to disconnect.
4. If you have to test multiple telephone user interfaces, repeat steps 1 through 3 to leave a call answer message for the next test subscriber.

Related topics:

[Performing acceptance tests for a new installation](#) on page 69

[Adding test subscribers](#) on page 69

[Retrieving test messages in integrated mode](#) on page 72

[Creating and sending a test message in non-integrated mode](#) on page 74

[Testing the outcalling capability](#) on page 75

[Creating and printing a fax message](#) on page 77

Retrieving test messages in integrated mode

Test the fully integrated operation of the system, as directed in this section. Use an extension for which you have access to the physical telephone.

Procedure

1. If MWI is started, check the message waiting indicator (MWI) on the test subscriber telephone. The MWI can be a light, a screen display, or a dial-tone stutter that you hear when you pick up the telephone.

 **Note:**

The message waiting lamp can take up to 1 minute to light on the appropriate telephone after a test message is sent.

If the MWI does not indicate that a message was received:

- a. Verify that the Mailbox Monitor and MWI services are started on the MAS.
 - b. To verify that the Mailbox Monitor and MWI services are started, double-click the **Monitor** icon on the desktop of the MAS designated as the MWI server, and then scroll down to these MM services in the right pane.
 - c. If the Mailbox Monitor or MWI service is stopped or if the Status column is blank, right-click the appropriate MM service and select **Start**.
 - d. Close this window.
 - e. Wait and re-validate.
2. If the Mailbox Monitor and MWI services are started, check for any problem in the following:
 - test subscriber administration. MWI service must be enabled both in the Class of Service and in Subscriber Options for the subscriber.
 - switch integration
 - switch number administration for the test telephone
 3. From the test subscriber telephone, dial the message retrieval number for the Modular Messaging system.
 4. Enter the password for this mailbox and press the pound key (#).
The system voices the name of the test subscriber.
 5. The first time you access this mailbox, you answer a series of prompts to set up the mailbox for operation. Answer all voice prompts as directed.
 6. After the mailbox is set up, retrieve the test message.
The system uses different commands to retrieve messages, depending on the type of user interface you use. Continue with the appropriate user interface.

7. To retrieve messages on the MM Aria interface.
 - a. Press **1 1** to review the new voice messages.
 - b. Listen to the test message. If the message does not play properly, contact the remote support center.
 - c. Press **7** to erase this message.
 - d. Repeat Steps b and c to review the next message, if any.
 - e. Press the star key (*) to return to the main menu.
 - f. Continue with Step 10.
8. To retrieve messages on the MM AUDIX interface.
 - a. Press **2** to review the new messages.
 - b. Press **0** to listen to the test message. If the message does not play properly, contact the remote support center.
 - c. Press star (*) **D**, or star (*) **3**, to erase this message.
 - d. Repeat Steps b and c to review the next message, if any.
 - e. Press star (*) **R**, or star (*) **7**, to return to the main menu.
 - f. Continue with Step 10.
9. To retrieve messages on the MM Serenade interface.
 - a. Press **5** to review the new messages.
 - b. Listen to the test message. If the message does not play properly, contact the remote support center.
 - c. Press **3** to erase this message.
 - d. Repeat Steps b and c to review the next message, if any.
 - e. Press the pound key (#) to return to the Ready menu.
10. Hang up the telephone to disconnect.
11. If MWI is installed, check the MWI on the test subscriber telephone. The MWI should be off. If it is not off, check the MWI administration on the MAS and the PBX.

Related topics:

[Performing acceptance tests for a new installation](#) on page 69

[Adding test subscribers](#) on page 69

[Leaving a call answer message](#) on page 71

[Creating and sending a test message in non-integrated mode](#) on page 74

[Testing the outcalling capability](#) on page 75

[Creating and printing a fax message](#) on page 77

Creating and sending a test message in non-integrated mode

The system uses slightly different commands for each telephone user interface. Note the differences in the text.

Procedure

1. Dial the message retrieval number for the Modular Messaging system from any telephone that is not administered on the system.
The system voices the Welcome to Avaya Messaging prompt.
2. Press the pound key (#) to skip the system introduction.
3. Enter the extension number for the test subscriber mailbox.
4. Enter the password for this mailbox and press the pound key (#).
The system voices the name of the test subscriber.
5. To create a new voice message:
 - On the MM Aria interface, press **2**.
 - On the MM AUDIX interface, press **1**.
 - On the MM Serenade interface, press **6**.
6. Speaking into the telephone, record the following or a similar test message after the tone: *This is a test voice mail message.*
7. Press the pound key (#) to approve the message.
8. When the system prompts you for the mailbox number, enter the mailbox number of another test subscriber. Then press the pound key (#).
The system voices the name of the test subscriber.
9. To approve the message and address list:
 - On the MM Aria interface, press the pound key (#) twice.
 - On the MM AUDIX interface, press the pound key (#).
 - On the MM Serenade interface, press the pound key (#) twice.
10. Press the pound key (#) again to send the test message to the test subscriber mailbox.
11. Hang up the telephone to disconnect.
12. Retrieve the message as described in Retrieving test messages in integrated mode.

Related topics:

[Performing acceptance tests for a new installation](#) on page 69

[Adding test subscribers](#) on page 69

[Leaving a call answer message](#) on page 71

[Retrieving test messages in integrated mode](#) on page 72


[Testing the outcalling capability](#) on page 75

[Creating and printing a fax message](#) on page 77

Testing the outcalling capability

Test the outcalling capability of the system:

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
2. Run the Modular Messaging Client software:
 - a. On the MAS, open Internet Explorer.
 - b. If the system displays a warning that the Internet Explorer Enhanced Security Configuration is enabled, click **OK**.
 - c. In the Internet Explorer main window, select **Tools > Internet Options**.
 - d. In the Internet Options window, click **Security** tab.
 - e. Click **Trusted Sites** so the item is highlighted, and then click **Sites**.
 - f. In the Trusted Sites window, verify that the **Require server verification (https:) for all sites in this zone** check box is clear.
 - g. Under Add this Web site to the zone, enter the full corporate computer name of the MSS and click **Add**. Use the format `mymss.loc.avaya.com`, for example, enter `mss.dr.avaya.com`.
 **Important:**
Do not enter `http://` or `https://` before the computer name, or the browser might not find the server automatically.
 - h. Click **OK** to close the Trusted Sites window.
 - i. Click **OK** to close the Internet Options window.
 - j. In the address field of the Internet Explorer main window, enter `http://mss1` the private address of the MSS and then press **Enter**. Use the format `mymss.loc.avaya.com`, for example, type `mss.dr.avaya.com`.
 - k. Continue logging in to the MSS.
3. Launch Subscriber Options:

- a. On the Messaging Administration web interface, Click **Messaging Administration > Subscriber Management**.
 - b. On the Manage Subscribers page, type a mailbox number into the **Local Subscriber Mailbox Number** field and click **Add** or **Edit**.
 - c. On the Edit Local Subscriber page, scroll to the bottom of the page and click **Launch Subscriber Options**.
 - d. On the File Download window, click **Open**.
4. Set up the recording and playback options to use a telephone near you:
- a. In the Modular Messaging User Properties window, click the **Media Setup** tab.
 - b. For When composing voice messages, select **Telephone**.
 - c. Click **Configure**.
 - d. In the Telephone Properties window, enter the extension number of a telephone near you.
 - e. Select or enter the name of this MAS if needed. Click **OK**.
 - f. For When reviewing voice messages, select **Telephone**.
 - g. Repeat Steps c through e to set up telephone playback.
 - h. Click **Apply**.
5. Record a personal greeting:
- a. In the Modular Messaging User Properties window, click the **Greetings** tab.
 - b. Ensure that the system uses the telephone to record and playback:
 - i. Check the icon to the left of the status display. If it shows a telephone, continue with Step c.
 - ii. If the icon shows a terminal, right-click and select **Telephone**. The icon changes to show a telephone. Continue with Step c.
 - c. Under Rules:
 - i. Under Default call handling, select **Play my personal greeting**.
 - ii. Click the red **Record** button on the player at the bottom of the window.
 - iii. When the telephone rings, answer the call and record a personal greeting for the test subscriber.
 - iv. After you record the test greeting, hang up the phone.
 - v. Click **Apply**.
6. Play back the greeting to test outcalling, as follows:

- a. Click the black, single-arrow **Play** button on the player near the bottom of the window.
 - b. Answer the telephone when it rings.
The picture of the telephone changes to off-hook.
 - c. Wait for the system to play the greeting recorded by the test subscriber.
 - d. Hang up the telephone.
The picture of the telephone changes back to being on-hook in two seconds.
7. Set up the MWI rule:
 - a. On the **Assistant** tab, right-click Message Waiting Indicator and click **New Rule**. Make sure that the option is checked.
 - b. Click the Message Waiting Indicator rule that appears. Text for the rule appears near the bottom of the tab.
 - c. Click **Apply**.
 8. Click **OK** to close the Modular Messaging User Properties window.
 9. Close all open windows.
-

Related topics:

[Performing acceptance tests for a new installation](#) on page 69

[Adding test subscribers](#) on page 69

[Leaving a call answer message](#) on page 71

[Retrieving test messages in integrated mode](#) on page 72

[Creating and sending a test message in non-integrated mode](#) on page 74

[Creating and printing a fax message](#) on page 77

Creating and printing a fax message

Procedure

1. From a fax machine, send a fax to the test subscriber mailbox. The subscriber's class of service must have both Inbound Fax and Outbound Fax Calls set to Yes.
2. Wait a few minutes for the fax to be delivered. The MWI lamp, if present on the test subscriber telephone should light up.
3. From a telephone (NOT the fax machine), dial the message retrieval number for the Modular Messaging system.
4. Press the pound key (**#**) to access the test subscriber mailbox.
5. Enter the extension number for the test subscriber mailbox.
6. Enter the password and press the pound key (**#**).

The system speaks the name of the test subscriber.

7. Retrieve and print the fax on the MM Aria interface as follows:
 - a. Press **1** to retrieve new messages.
 - b. Press **3** to retrieve the fax message.
 - c. After the prompts, press **2** and follow the prompts.
8. Retrieve and print the fax on the MM AUDIX interface as follows:
 - a. Press **2** to retrieve new messages.
 - b. Press star (*) **1** to print the fax.
 - c. Press star star (**) **6** and follow the prompts.
9. Retrieve and print the fax on the MM Serenade interface as follows:
 - a. Press **1 9** to retrieve new messages.
 - b. Press **8** to print the fax.
 - c. Press **3** and follow the prompts.
10. Verify that the fax prints correctly.
11. If MWI is installed, check the MWI on the test subscriber telephone again. The MWI lamp should be off.

Related topics:

[Performing acceptance tests for a new installation](#) on page 69

[Adding test subscribers](#) on page 69

[Leaving a call answer message](#) on page 71

[Retrieving test messages in integrated mode](#) on page 72

[Creating and sending a test message in non-integrated mode](#) on page 74

[Testing the outcalling capability](#) on page 75

Removing the test subscribers on the MSS

Before you remove the test subscribers, ensure that you complete any other testing, such as ELA or Broadcast testing. When the acceptance testing is complete, remove the test subscribers:

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
 2. From the Messaging Administration Web interface, click **Subscriber Management**.
The system displays the Manage Subscribers page.
 3. On the line Local Subscribers for this MSS, such as *mymss*, click **Manage**.
 4. On the Manage Local Subscribers page:
 - a. Select the test subscriber to delete.
 - b. Click **Delete the Selected Subscriber**.
 - c. If the system prompts you to confirm removing the subscriber, click **OK**.
 - d. At the confirmation prompt, click **OK**.
 5. Repeat Step 4 to remove all test subscribers.
-

Performing acceptance tests for a new installation

Chapter 9: Setting up alarming

Configuring the system alarms

You must configure the alarms after installing Modular Messaging.

Procedure

To configure the system alarms, send the *Universal Install Product Registration Request Form* to the registration team.

The Avaya Registration team will make the appropriate changes to allow access to your managed devices through the SAL Gateway.

You will receive an e-mail from Avaya to confirm that remote access to the Modular Messaging system has been enabled through your SAL Gateway.

Setup alarming on the MSS

This section provides information about how to administer alarm notification for your Modular Messaging system.

The MSS generates system alarms and error logs that you can gain access to by using the MSS Web Administration forms. The MAS generates system alarms and error logs that you can gain access to by using a command line interface tool. This command line interface tool is called `displot` on the MAS. Notifications that alarms generate can be sent to any one of the following recipients:

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



Note:

Partners need access to the Modular Messaging system to receive these notifications.

- Avaya Fault and Performance Manager with use of either Secure Services Gateway (SSG) or Avaya Proxy Agent

Specifying MSS alarm origination

Activate alarm origination to enable the appropriate party to receive notification of alarms that occur on the system.

About this task

To set up alarm origination through the MSS:

Procedure

1. Connect to the MSS. For more information, see [Accessing the MSS using the MSS Web console](#) on page 35.
2. If there is a notification of active alarms, then follow the process described in the *MSS alarms* available on <http://www.avaya.com/support> to clear these alarms.
3. From the **Alarming** menu, click **Alarming Configuration**.
The system displays the Configure Alarms page.
4. Enter the **Product ID** for the MSS.
5. Set the **Alarm Origination** to SAL or INACTIVE.
6. Verify that **Alarm Suppression** is set to **INACTIVE**. You can use the default settings for **Alarm Level** and **Clear Alarm Notification**. For more information about completing each field, click **Help**.
7. Complete the alarming information for the site:
 - a. Click **Save** on the Configure Alarms page.
 - b. From the **Alarming** menu, select **SNMP Community**.
 - c. On the Administer SNMP Community page, click **Add** to add the community you need for SNMP trap destination. If the community already exists, skip to step g.
 - d. For **Community**, click the field and enter a community name. This name is used to validate when communicating between the SNMP client and the SNMP server on the System Platform.
 - e. For **Apply To**, from the drop-down menu, select either **Traps** or **Both**.
 - f. Click **Save**, a window appears if the add was successful.

- g. From the **Alarming** menu, click **SAL Destinations**.
 - h. Click **Add**.
 - i. Complete the appropriate fields. For more information about completing each field, see the SAL Destinations setup in the task [Configuring serviceability settings on MAS](#) on page 83.
 - j. Click **Save**.
-

Configuring serviceability settings on MAS

You must setup domain wide serviceability (alarming) settings once for Modular Messaging system.

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
 2. In the Voice Mail System Configuration window, double-click **Serviceability**. The system displays the Serviceability - Voice Mail Domain window.
 3. On the **General** tab, click **SAL** to send alarms to an NMS using an agent gateway. If you select **Inactive**, Modular Messaging system does not send any alarm notification.
 4. On the **SAL destinations** tab, complete the following:
 - a. For **IP Address/Host**, enter the IP address or FQDN for the SAL gateway.
 - b. For **Community**, select a community name. This name is used as a security validation for communications between the SAL client and the SAL server.
 - c. For **Port**, enter the port number.
 5. Click **OK** to close the Serviceability - Voice Mail Domain window.
-

Testing alarming origination

For alarming setups, test the alarm origination to verify that alarms are logged correctly and are sent to the correct destination.

About this task

To test the alarm origination:

Procedure

1. Connect to the MSS. For more information, see [Accessing the MSS using the MSS Web console](#) on page 35.
 2. From the **Diagnostics** menu, click **Alarm Origination**.
The system displays the Test Alarm Origination page.
 3. Click **Run Test**.
 4. Wait for five minutes for the test alarm to be acknowledged and resolved.
 5. Access the Alarm Log. From the **Logs** menu, click **Alarm**.
 6. On the Alarm Log page, click **Display** to determine if the minor alarm VM type ALARM_ORIG is still active. If the alarm is resolved before 30 minutes has elapsed, consider that the alarm is working. If during the 30 minutes the alarm is still active:
 - a. Click **Back** on the Web browser.
 - b. Wait a few more minutes, and then click **Display** again.
 7. When the active alarm no longer appears in the alarm list:
 - a. On the Alarm Log page, set the **Alarm Type** to **Resolve**.
 - b. Click **Display**.
 - c. Locate the **VM** alarm type **ALARM_ORIG** at alarm level **MIN**. Verify that the alarm was acknowledged with a **Y** in the **Ack** column, and resolved.
 8. If the test fails, that means the alarm only cleared after a reboot or after 30 minutes had elapsed (the MAINT process clears the alarm automatically after 30 minutes), verify that the remote service center is connected. Correct any settings, and test the alarm.
-

Chapter 10: Creating snapshot of the MAS

Taking snapshot of the MAS

Use the following procedure on Dom0 to create a snapshot of the guest domain of the MAS. In case of any failure/corruption of MAS in the future, this snapshot can be used to restore the MAS to its initial install state without restoring the MSS.

Procedure

1. Log in as *root* on dom0.
 2. Type the following to create the snapshot as a new logical volume:


```
lvcreate --size 20G -s -n mas1snap /dev/VolGroup00/lv_mas1
```
 3. Type the following to create the logical volume for the backup file:

```
lvcreate --size 15G -n mas1backup /dev/VolGroup00
```
 4. Type the following to format the logical volume as EXT3:

```
mkfs.ext3 /dev/VolGroup00/mas1backup
```
 5. Type the following to mount the volume:

```
mkdir /mnt/tmpBackup  
mount /dev/VolGroup00/mas1backup /mnt/tmpBackup
```
 6. Type the following to DD and gzip up the file system:

```
dd if=/dev/VolGroup00/mas1snap | gzip -1 > /mnt/tmpBackup/  
lv_mas1.dd.gz
```

 **Note:**
gzip -1, where “1” is “One”
 7. Type the following to unmount the *mas1backup* file system:

```
umount /mnt/tmpBackup
```
 8. Type the following to remove the snapshot volume to free up the space:

```
lvremove /dev/VolGroup00/mas1snap
```
-

Restoring the MAS from the snapshot

Procedure

Contact Avaya services or Avaya Partner to restore the MAS from the snapshot.

Chapter 11: Backing up the system

Backing up the system

As a final installation task, back up the information that you administered on the system.

Single server configuration provides only LAN based backup. Administrators can back up MAS and MSS data on a remote storage location on the LAN. LAN backups facilitate disaster-recovery and allows you to make a complete backup for large systems with many subscribers and messages. If a system failure occurs, the backup data stored on the remote storage location on the LAN is used to restore the system to an operational state.

Procedure

1. Log on to the System Platform Web Console.
2. Click **Server Management > Backup/Restore**.
3. Back up the System Platform data. For more information, see the *Administering Avaya Aura® System Platform* guide.
4. Use the Data Collection Tool (DCT) to gather and analyse data from the MAS. For more information, see [Using the DCT to analyze the current configuration](#) on page 88.
5. Caller Applications (*.uma files), once deployed, are stored on the MAS within a folder that has a GUID. The location for this folder is `C:\Program Files\Avaya Modular Messaging\VServer\CallerApps`. Avaya recommends that you back up a copy of this folder.

Deployed caller applications cannot be backed up using NTBackup while the Modular Messaging (MM) Messaging Application Server service is running. However, you can make a copy of the CallerApps folder while this service is running, and then make a backup of that (you could choose to create scripts to carry out this function).
6. Before you back up the MAS, verify that all spooled messages are delivered. For more information, see [Checking the spool folder on the MAS](#) on page 89.
7. Back up MAS and MSS data on a remote storage location on the LAN. For more information, see [Running backups on the MAS](#) on page 89 and [Backing up the MSS](#) on page 92.

Using the DCT to analyze the current configuration

You must ensure that the DCT file for the Avaya Modular Messaging system is complete and current. Obtain the latest recommended DCT file from the Avaya support Web site (<http://www.avaya.com/support>).

Procedure

1. Verify that the Modular Messaging system is working correctly and all servers are running.
2. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
3. In Windows Explorer, navigate to the directory that contains the DCT program. You can find a copy of the DCT executable file in **C:\Program Files\Avaya Modular Messaging\Install\MISCM**.
4. Double-click **MMDCT.exe**
5. In the Avaya Modular Messaging Data Collection Tool window, select **Analyze existing system**, and then click **OK**.
6. When the program asks if you want to use an existing DCT file, click **Yes**.
7. In the Open window, click the drop-down list next to **Look in**.
8. Navigate to C:\Program Files\Avaya Modular Messaging\Install\MISCM\cfg folder and locate the *VSPDCT.mmdct* file.
9. Double-click the *VSPDCT.mmdct* file.
10. On the MM System Analysis screen, use the **MAS Information is being collected from** drop-down menu to select the MAS1.
11. Click **Start**.
The system displays the data collection process in the window. After the information is collected successfully, which could take several minutes, the system displays a confirmation window.
12. Click **OK**.
13. On the Avaya Modular Messaging Data Collection Tool window, click **Save**.
14. In the Save As window, navigate to C:\Program Files\Avaya Modular Messaging\Install\MISCM\cfg folder.
15. Type the name of the file in the **File name** field as backup to indicate that it is a backup DCT file.
16. Click **Save**.

17. On the Avaya Modular Messaging Data Collection Tool window, click **Cancel**.
 18. Click **No** when asked to save the current configuration (you already saved the file above).
-

Checking the spool folder on the MAS

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
 2. Open Windows Explorer.
 3. Navigate to the folder **C:\Program Files\Avaya Modular Messaging\Server\Spool**.
 4. Make sure that the Spool folder contains no message files.
-

Running backups on the MAS

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
2. Log on to the same account that you used on the Windows Domain Setup page for placing the MSS in a Windows domain.
 - In a private Windows domain, use the domain administrator account name, such as *dom-admin*.
 - In a corporate Windows domain, use the customer account name, such as *custacct*.
3. To view the scheduled backup program for the MAS, double-click the Scheduled Tasks icon on the desktop.
4. In the Scheduled Tasks window, run an attended backup on this MAS:
 - a. Right-click the task named MAS Backup and select **Run**.

The system immediately starts to back up the data on this MAS to the MSS. The **Status** column shows **Running**. When the backup is complete, the **Status** column goes blank. This process takes about a minute.

When the backup completes successfully, continue with Step 6.

- b. Optional: To verify if the backup process is successful.
 - a. Double-click the **Monitor** icon on the desktop.
 - b. In the left pane, expand Event Viewer (Local), and then click **Application**.
 - c. Refresh the window display periodically until you see the following events.
 - ntbackup 8009, End Verify: The operation was successfully completed.
 - ntbackup 8019, End Operation: The operation was successfully completed.
 5. If the backup fails to run, verify the account settings.
 - a. Double-click the task **MAS Backup** to view the properties window.
 - b. In the MAS Backup window, click the **Task** tab. Verify that the account in the Run as field is the correct account that has permissions to run backups manually. If the account is incorrect, you can type the correct value now.
 - c. If you change the account, or if you want to verify the password, click **Set Password**. In the Set Password window, enter and confirm the password for the required account. Click **OK**.
 - d. Click **OK** to close the MAS Backup window.
 - e. Repeat Step 4–a to run the backup again.
 6. Close the Scheduled Tasks window.
-

Restoring backed-up MAS data

Restore the data on the MAS from the most recent backup. Data includes any customized caller applications, prompts, and tone files.

About this task

To restore the backed-up MAS data:

Procedure

1. Map to the backup drive for this MAS on the MSS:
 - a. On the desktop, right-click the **My Computer** icon and select **Map Network Drive**.

 **Note:**

If you renamed the icon label, the computer icon shows the server name, such as *mymas1*.

- b. In the Map Network Drive window, in the **Folder** field, type \\
mss1\masbackup.
 - c. Clear the **Reconnect at logon** check box.
 - d. Click **Connect using a different user name**.
 - e. In the Connect As window, for **User name**, enter the private Windows domain name and the domain administrator account name in the format `domain\account name`. For example, type `privdom1\dom-admin`.
 - f. Enter the password for this account. Click **OK**.
 - g. In the Map Network Drive window, click **Finish**.
The system opens a window to the designated drive letter, such as Z:.
2. Double-click the **Backup** icon on the desktop.
 3. In the Backup Utility window, on the **Welcome** tab, click **Restore Wizard**.
 4. On the Welcome screen for the Restore Wizard, click **Next**.
 5. On the What to Restore screen, click **Browse**.
 - a. In the Open Backup File window, click **Browse**.
 - b. In the Select file to catalog window, under **Look in**, navigate to the mapped drive.
 - c. Double-click the backup file for this MAS. which has the name like , `<computername>MASSingle.bkf`, where `<computername>` is the netbios name of the MAS.
 - d. In the Open Backup File window, click **OK**.
The system returns to the What to Restore screen.
 6. Verify that the system displays the full name of the MAS backup file in the right pane under Media Location. For example, `Z:\MYMAS1MASSingle.bkf`.
 7. In the left pane under **Items to restore**, expand **File**.
 - a. Expand the correct entry for the daily backup of this MAS. The file uses the naming convention from the previous software release, such as *Daily Backup of MYMAS1*.
 - b. Expand C:.
 8. Select the folders and files to be restored:
 - a. Select the **Avaya_Support** check box. This folder includes the **Tone_Files** folder, which contains any custom tone files.
 - b. Expand the folders **Program Files > Avaya Modular Messaging > VServer**.
 - c. Select the **VServer** check box.

 **Caution:**

Do not restore the System State! You also do not need to restore the hosts file, because you already resent the most current version from the MSS.

- d. Click **Next**.
9. On the Completing the Restore Wizard screen, click **Advanced**.
 - a. On the Where to Restore screen, select **Original location**. Click **Next**.
 - b. On the How to Restore screen, select **Replace existing files**. Click **Next**.
 - c. On the Advanced Restore Options screen, verify the following settings:
 - Clear the **Restore security setting** check box and the **Restore junction points, not the folders and file data they reference** check box.
 - Leave the **Preserve existing volume mount points** check box selected.
 - Click **Next**.
10. On the Completing the Restore Wizard screen, review the restore information. Click **Finish**.

The Restore Progress window displays restore information.
11. When the data restoration is complete, close the Restore Progress window.
12. Close the Backup Utility window.
13. If the system asks if you want to restart, select to restart.
14. Close the mapped drive window, such as **Z:**.

 **Caution:**

You must disconnect the mapped drive, or automatic nightly backups might fail.

15. Disconnect the mapped drive:
 - a. On the desktop, right-click the **My Computer** icon and select **Disconnect Network Drive**.
 - b. In the Disconnect Network Drives window, under **Network Drives**, select **\mss1\masbackup**. Click **OK**.

Backing up the MSS

After you back up the MAS to the MSS, back up all data from the MSS to the LAN.

Procedure

1. Connect to the MSS using MSS Web console. For more information, see [Accessing the MSS using the MSS Web console](#) on page 35.
 2. Log on to the MSS server as **sa**.
The system displays the Messaging Administration main menu.
 3. Verify the number of subscribers:
 - a. From the Messaging Administration menu, click **Subscriber Management**.
 - b. Make a note of the number of subscribers.
 4. Stop the messaging service:
 - a. From the Utilities menu, click **Stop Messaging**.
The system opens the Stop Messaging Software page.
 - b. Click **Stop**.
 5. After the system reports that the voice system has completely stopped, begin an attended backup:
 - a. From the **Backup/Restore** menu, click **Backup**.
 - b. On the **Backup** page, set all data types to **Yes**.
 - c. Click **Save** or **Start Backup**.
 - d. If the system opens an SSH Authorization window, log in as **sa**.
 - e. Click **Continue**.
 6. The system saves the new system configuration to the LAN.
 7. Follow the prompts on the screen to track and complete the backup process. Scroll to the bottom of the page to see the most recent status messages. The message **FULL-MANUAL BACKUP** completed successfully indicates that the backup is complete.
-

Backing up the system

Chapter 12: Restoring the system

Recovering the system

 **Note:**

If you are recovering only the Modular Messaging system, then you are not required to install the System Platform.

Procedure

1. Install the System Platform. For more information, see [Install System Platform](#) on page 20.

 **Note:**

Ensure that you install the System Platform with the latest patches.

2. Install the Modular Messaging template. For more information, see *Chapter 5: Installing Avaya Modular Messaging*.

 **Note:**

Avaya recommends that you use the same EPW file that you used for the initial install. All the networking data including the host names and domain names on this new install has to be same as in the previous install.

3. Install the latest available software updates on the MAS, the MSS and the Web Client server. For more information, see *Chapter 7: Updating Modular Messaging*.
4. Restore the System Platform data on CDOM. For more information, see the *Administering Avaya Aura® System Platform* guide.
5. Restore data on the MSS. For more information, see [Restoring data on the MSS](#) on page 96.

 **Note:**

Make sure that the correct number of subscribers and the networking settings for the MSS got restored.

6. Take the backed up DCT file from the backup folder and copy it on the MAS.
 - a. Copy the backed up DCT file to `C:\Program Files\Avaya Modular Messaging\Install\MISCM\cfg\backup.mmdct`.

- b. Open command prompt using Windows Run dialog. Type *cmd* on Windows **Run** dialog and hit enter.
- c. Navigate to `C:\Avaya Support\Scripts`.
- d. Run the following command from command prompt

```
cscript RestoreRegistry.vbs -BACKUPDCT "C:\Program Files
\Avaya Modular Messaging\Install\MISCM\cfg\backup.mmdct"
-MASNUM 1
```

In the above command replace `backup.mmdct` with the backed up DCT file name and `-MASNUM` argument with the current MAS number on which the restore is being performed.

The system copies the registry data from the backed up DCT to the registry hive.

7. Restart the messaging services. For more information, see [Restarting the messaging services](#) on page 98.
 8. Install the latest anti-virus software. For more information, see [Installing and administering anti-virus software](#) on page 50.
 9. Verify and update all required VMSC settings. For more information, see [Completing VMSC setup](#) on page 100.
 10. Complete the MSS administration. For more information, see [Completing MSS administration](#) on page 100.
 11. Restore the data on the MAS from the most recent backup. For more information, see [Restoring backed-up MAS data](#) on page 90.
 12. Restore the caller applications. For more information, see [Restoring Caller Applications](#) on page 103.
-

Restoring data on the MSS

To restore data on the MSS:

Procedure

1. Connect to the MSS. For more information, see [Accessing the MSS using the MSS Web console](#) on page 35.
2. Stop the messaging service:
 - a. From the Utilities menu, click **Stop Messaging**.
 - b. On the Stop Messaging Software page, click **Stop**.
The system displays the status of stopping the messaging system.

3. Setup the remote storage configuration.
4. After the system reports that the voice system has completely stopped, start the data restoration:
 - a. From the **Backup/Restore** menu, select the backup to restore and click **Restore**.
 - b. On the Restore page, set all the data types to **Yes**.
 - c. Click **Start Restore**. When you see the overwrite warning, click **OK**.
The system starts restoring all data to the system. To follow the progress of the data restoration, press Page Down or scroll down to see the bottom of the screen.
5. After the restore is complete, reboot the system.
 - a. Click **Reboot**.
 - b. Wait for 3 minutes and refresh the page.
6. At the prompt, log on to the MSS as **sa**.
The server displays the Messaging Administration web interface.
7. As a sanity check, display the Configure Network Addressing page:
 - a. From the **Server Administration** menu, click **TCP/IP Network Configuration**.
 - b. Verify the settings on this page. Verify that the corporate and private LANs are not backward.
8. From the Messaging Administration web interface, click **Subscriber Management**:
 - a. Verify that the correct number of subscribers is restored. You recorded this number before backing up the MSS.
 - b. On the **Manage Classes-of-Service** page, verify that the classes of service are correctly restored.
9. The system does not back up passwords for the remote-access login accounts. You must re-enter the correct passwords to enable remote access.
 - a. From the **Security** menu, click **Local Administrators**.
The system displays the Manage Local Administration Accounts page.
 - b. Select an account, such as sa or vm, and then click **Edit the Selected Admin**.
The system displays the Edit Local Administration Account page.
 - c. From the **Local Authentication Enabled?** drop-down menu, select **yes** (if it is not already selected).
 - d. In the **Password** field, enter the appropriate password.
 - e. In the **Confirm Password** field, enter the password again for verification.
 - f. Click **Save**.

- g. Repeat Step *b* for each additional login that you must administer.
- h. Set the administrative password defaults (**sa** and **vm**) and give the passwords to the customer.

Restarting the messaging services

Procedure

1. Connect to the MAS. For more information, see [Accessing the MAS using RDC](#) on page 35.
2. Click **Services (Local)** in the left pane, if the item is not already selected.
3. Restart messaging service to enable any changes you made in the VMSC:
 - a. Select **MM Messaging Application Server**.
 - b. Right-click and select **Stop**.
 - c. When service is stopped, right-click MM Messaging Application Server again and select **Start**. The system restarts the messaging service. When you restart the messaging service, the Monitor window immediately shows the status as **Started**. However, the service might actually take several minutes to start. The time it takes depends on the number of port boards installed and the integration method. Track the status as follows:
 - d. In the left pane, expand **Event Viewer (Local)**, and then click **Application**.
 - e. Refresh the window display periodically until you see **Telephony User Interface** event 1241, **TUI service has been enabled**. You can then proceed.
4. Verify that the Modular Messaging services required for the MAS are started:
 - a. In the Monitor window, select **Services (Local)** in the left pane.
 - b. In the right pane, scroll down to the list of Modular Messaging services. These services start with the abbreviation **MM**. Verify that the **Status** column shows the correct state for each messaging service:
 - The following services are automatically installed on the MAS. Enable them based on the information in the table.

Modular Messaging service name	Condition for enabling service
MM Messaging Application Server MM Service Connector Apache Tomcat	Enable on the MAS. Apache Tomcat service must be enabled on the server on which

Modular Messaging service name	Condition for enabling service
Avaya Diagnostic Tools Avaya SPIRIT MM Alarming Server MM Audit Service MM Event Monitor Server MM Fault Monitor MM Performance Monitor Server MM Process Monitor Server	WebLM server is installed. Apache Tomcat is not a Modular Messaging service.
MM Call Me MM Fax Sender MM Mailbox Monitor MM MWI MM Tracing Service	Enable the service on the MAS for the feature that you are using.

- Services that are required for this server must show **Started** and a startup type as **Automatic**.
 - Services that are not required on this server must show a blank status and a startup type as **Disabled**.
- c. If the **Startup Type** for any MM service that is not required for this server is Manual:
- i. Double-click the service to open the Properties window.
 - ii. Set the **Startup Type** to **Disabled**.
 - iii. Click **OK**.
 - iv. Refresh the screen to verify that all **MM** services that are not required for this server are **Disabled**. Repeat for each service as needed.
- d. If the **Status** for any MM service that is required for this server is Stopped or blank:
- i. Click **Start > Run** to open the Run window.
 - ii. In the **Open** field, type the following and press **Enter**:

```
C:\Avaya_Support\Scripts\serverrecovery.vbs
```

The script takes a few seconds to run. The program sets up all MM services correctly.
 - iii. Refresh the screen to verify that all MM services required for this server are **Started** and set to **Automatic**.
 - iv. If any required MM services are not set up correctly, repeat Step d.
5. When configuration is complete, close all open windows.
-

Completing VMSC setup

About this task

Complete the following for the MAS:

Procedure

1. Enter product IDs for the MAS. For more information, see [Entering Product ID for the MAS](#) on page 53.
 2. Configure the SAL destinations and community details using the Serviceability - Voice Mail Domain window of the Voice Mail System Configuration program. For more information, see [Configuring serviceability settings on MAS](#) on page 83.
 3. Configure the required services. For more information, see [Configuring specific features as needed](#) on page 54.
-

Completing MSS administration

To complete MSS administration:

Procedure

1. Connect to the MSS. For more information, see [Accessing the MSS using the MSS Web console](#) on page 35.
2. Complete the following tasks on the MSS:
 - Verify the MAS host information
 - Placing the MSS in the Windows domain

For instructions to complete MSS administration, see *Completing MSS administration* chapter in the *Avaya Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Release 5.2 Installation and Upgrades* guide.

3. Reboot the MSS.
-


Restoring backed-up MAS data

Restore the data on the MAS from the most recent backup. Data includes any customized caller applications, prompts, and tone files.


About this task

To restore the backed-up MAS data:

Procedure

1. Map to the backup drive for this MAS on the MSS:
 - a. On the desktop, right-click the **My Computer** icon and select **Map Network Drive**.
 **Note:**
If you renamed the icon label, the computer icon shows the server name, such as *mymas1*.
 - b. In the Map Network Drive window, in the **Folder** field, type `\mss1\masbackup`.
 - c. Clear the **Reconnect at logon** check box.
 - d. Click **Connect using a different user name**.
 - e. In the Connect As window, for **User name**, enter the private Windows domain name and the domain administrator account name in the format `domain\account name`. For example, type `privdom1\dom-admin`.
 - f. Enter the password for this account. Click **OK**.
 - g. In the Map Network Drive window, click **Finish**.
The system opens a window to the designated drive letter, such as Z:.
2. Double-click the **Backup** icon on the desktop.
3. In the Backup Utility window, on the **Welcome** tab, click **Restore Wizard**.
4. On the Welcome screen for the Restore Wizard, click **Next**.
5. On the What to Restore screen, click **Browse**.
 - a. In the Open Backup File window, click **Browse**.
 - b. In the Select file to catalog window, under **Look in**, navigate to the mapped drive.
 - c. Double-click the backup file for this MAS. which has the name like `<computername>MASSingle.bkf`, where `<computername>` is the netbios name of the MAS.

- d. In the Open Backup File window, click **OK**.
The system returns to the What to Restore screen.
6. Verify that the system displays the full name of the MAS backup file in the right pane under Media Location. For example, *Z:\MYMAS1MASSingle.bkf*.
7. In the left pane under **Items to restore**, expand **File**.
 - a. Expand the correct entry for the daily backup of this MAS. The file uses the naming convention from the previous software release, such as *Daily Backup of MYMAS1*.
 - b. Expand C:.
8. Select the folders and files to be restored:
 - a. Select the **Avaya_Support** check box. This folder includes the **Tone_Files** folder, which contains any custom tone files.
 - b. Expand the folders **Program Files > Avaya Modular Messaging > VServer**.
 - c. Select the **VServer** check box.

 **Caution:**
Do not restore the System State! You also do not need to restore the hosts file, because you already resent the most current version from the MSS.

 - d. Click **Next**.
9. On the Completing the Restore Wizard screen, click **Advanced**.
 - a. On the Where to Restore screen, select **Original location**. Click **Next**.
 - b. On the How to Restore screen, select **Replace existing files**. Click **Next**.
 - c. On the Advanced Restore Options screen, verify the following settings:
 - Clear the **Restore security setting** check box and the **Restore junction points, not the folders and file data they reference** check box.
 - Leave the **Preserve existing volume mount points** check box selected.
 - Click **Next**.
10. On the Completing the Restore Wizard screen, review the restore information. Click **Finish**.
The Restore Progress window displays restore information.
11. When the data restoration is complete, close the Restore Progress window.
12. Close the Backup Utility window.
13. If the system asks if you want to restart, select to restart.
14. Close the mapped drive window, such as **Z:**.

 **Caution:**

You must disconnect the mapped drive, or automatic nightly backups might fail.

15. Disconnect the mapped drive:
 - a. On the desktop, right-click the **My Computer** icon and select **Disconnect Network Drive**.
 - b. In the Disconnect Network Drives window, under **Network Drives**, select **\mss1\masbackup**. Click **OK**.
-

Restoring Caller Applications

About this task

If Caller Applications were installed on the system, run the Caller Applications restore script:

Procedure

1. Click **Start > Run** to open a Command prompt window.
 2. In the Run window **Open** field, type the following and press **Enter**:
`c:\Avaya_Support\CMD\CARestore.bat`
A command window opens. The script shuts down all Modular Messaging services, and copies the Caller Applications to the server. The script takes a few seconds to run.
-

Chapter 13: Troubleshooting

Template installation summary shows errors

Solution:

- Ensure that the IP address and machine name specified for the MAS, MSS, or WC machine do not exist on the network.
- In case of corporate domain, ensure that the *cust* account and the *tech support* account specified during installation exist in the domain administrators group.
- Ensure that the license key specified during the installation is valid.
- In case of corporate domain, ensure that the CDOM time and the time zone matches with the corporate network time and time zone.

Insufficient resources to install the template

Problem:

You get the following error while installing Modular Messaging.

Insufficient resources to install this template (Insufficient disk space left on */vsp-template*. (Requested=10124MB Available=5295MB)).

Cause:

Template is already available on CDOM.

Solution:

You can do one of the following:

- If the template is the correct version of the template that you are trying to install,
Use the **SP Server** option from the System Platform Web Console to install the template. For more information, see [Locating templates](#) on page 38.
- If the template is not the correct version of the template that you are trying to install,
 - Remove the template. You can remove the template from the System Platform Web Console (**Server Management > File Manager**).

- Obtain the new template. For more information, see, [Obtain a Modular Messaging template](#) on page 20.
- Install the template.

Template installation complete but there are lines in the template installation log, which says 'with problem finished mss configuration'

Follow these steps to solve this problem:

1. Open the MSS Web console.
2. Under **Logs**, open the DCT configuration log.
3. Read the last error message and take appropriate action depending on the error message as mentioned below:

- Failed to perform MAS Host Setup configuration.

In case of corporate domain, ensure that the *cust* account specified in the template configuration exists in the Domain administrators group in the specified domain.

- Failed to create system subscribers, you cannot perform this operation without valid license.

Ensure the time and time zone on the System Platform server matches with the network time and time zone.

- Failed to set host name.

Ensure the host name you have specified is unique in the network.

Template installation completed but last status message says mas: ConfigCredentialLDAP FAILED

Cause:

MSS configuration failed, therefore MAS could not join the MSS.

Solution:

To know where the template installation failed, follow these steps:

1. In the MSS weconsole, type `http://mss-name`.
2. Under **Logs**, click the **MSS DCT Configuration Logs** hyperlink.

The last log message indicates the step at which the template installation failed.

System Platform Web Console does not update information for long time

Cause:

System Platform Web Console updates information only when some configuration state is complete. If a step takes long time to complete, System Platform Web Console may not update anything for that time.

Solution:

The following conditions indicate that the license key you provided was invalid:

- System Platform Web Console does not update MAS or WC/WSO configuration logs for long time
- Last log message is Xen Net Device Driver or there is no log message regarding sysprep

To correct this, access the MAS and WC/WSO using VNC, and then enter a valid license key.

How to know if the configuration was successful?

Click **Virtual Machine Management > View Installation/Upgrade Log** from the System Platform Web Console.

The last lines of logs should read:

- mss:Finished Windows Domain Setup
- mss configuration finished
- Finished

Appendix A: Planning form for installing Modular Messaging

As part of the installation of Avaya Modular Messaging, you are required to supply specific configuration information. This form will help you to gather the information required to complete a successful installation.

Print out the following tables and work with your network administrator to fill in the rows.

For detailed field descriptions, see Appendix B: Field descriptions of planning form for installing Modular Messaging.

Table 1: Corporate Network Details / Domain Name Servers

Field	Value/requirement	Notes
Subnet Mask		
Default gateway		
Default DNS server		
DNS server address 2		Optional
DNS server address 3		Optional
DNS suffixes (separate multiples by commas)		Optional

Table 2: Corporate Modular Messaging details

Field	Value/requirement	Notes
MSS IP address		
MAS IP address		
MSS Full computer name (FQDN)		
MAS Full computer name (FQDN)		

Table 3: Windows domain configuration

Field	Value/requirement	Notes
Join a Private windows domain?	Yes / No	
Join a Corporate domain?	Yes / No	
Windows domain name		In case of private domain For example, MM.local
Domain controllers host name (FQDN)		In case of corporate domain
Corporate windows domain name (FQDN)		In case of corporate domain

Table 4: Modular Messaging configuration

Field	Value	Notes
Mailbox number length		
MAS Windows license key		
VMD name		
Web Client server IP		Required only if Web Client is installed on the System Platform
Web Client server FQDN		Required only if Web Client is installed on the System Platform
Web Client Windows license key		Required only if Web Client is installed on the System Platform
Language used for announcement and TTS		

Table 5: Modular Messaging accounts - MSS account info

Field	Value/requirement	Notes
MM login "sa" password		
MSS login "vm" password		

Field	Value/requirement	Notes
Trusted servers password		

Table 6: Modular Messaging accounts - MAS login accounts & passwords

Field	Value/requirement	Notes
Technical support logon name		In the case of a corporate domain setup this must be available in the domain administrator's list before installation.
Technical support password		
Customer account logon name		In the case of a corporate domain setup this must be available in the domain administrator's list before installation.
Customer account password		
MAS local administrators account user name		
MAS local administrators account password		

Table 7: Switch integration information

Field	Value/requirement	Notes
Switch name (PBX)		
SIP Domain (FQDN)		
SIP gateway address		

Table 8: Product registration information

Field	Value/requirement	Notes
Host name - MSS		
IP address - MSS		

Planning form for installing Modular Messaging

Field	Value/requirement	Notes
Host name - MAS		
IP address - MAS		
Host name - Web Client		
IP address - Web Client		
Customer name		
Avaya Sold-to number		
Contact details		

Appendix B: Field descriptions of planning form for installing Modular Messaging

Corporate Network Details field descriptions

Name	Description
Subnet mask	When using static IP addressing, specifies the subnet mask for the subnet on which the MSS resides. The subnet mask must be in the range 128 . 0 . 0 . 0 to 255 . 255 . 255 . 254. The uppermost bit of the subnet mask must be a 1. The lowest bit must be a 0. For example, 255 . 255 . 255 . 0 is valid, but 0 . 255 . 255 . 255 and 255 . 255 . 255 . 255 are not valid.
Default gateway	Specifies the IP address of the default gateway for the LAN or subnet where the MSS resides.

Related topics:

[Setting up the network](#) on page 41

Domain Name Servers field descriptions

Name	Description
Default DNS Server	The default DNS server specifies the IP address of the first DNS server used by Modular Messaging MAS. This information is used to resolve the computer names to the IP addresses.

Name	Description
DNS Server address 2	(Optional) The DNS server address 2 specifies the IP address of the secondary DNS server used by Modular Messaging MAS. This information is used to resolve the computer names to the IP addresses.
DNS Server address 3	(Optional) The DNS server address 3 specifies the IP address of the third DNS server used by Modular Messaging MAS. This information is used to resolve the computer names to the IP addresses.
Append these DNS suffixes, separated by commas.	Separates the suffixes using a comma. It specifies the name of each DNS domain to search in the order of use. The search order is from the top of the list down.

Related topics:

[Setting up the network](#) on page 41

Corporate MM networking field descriptions

Name	Description
MSS IP Address	The IP address of the server on which the MSS is installed. You must assign a static IP address to the MSS.
MAS IP Address	The IP address of the server on which the MAS is installed.
MSS Full Computer Name	The Fully Qualified Domain Name of the server on which the MSS is installed. The fully qualified domain name (computer plus domain name) must be 64 or fewer characters. Use only lower-case alpha characters, numbers, and the hyphen character (-). The first character cannot be a number.
MAS Full Computer Name	The Fully Qualified Domain Name of the server on which the MAS is installed. The fully qualified domain name (computer plus domain name) must be 64 or fewer characters. Use only lower-case alpha characters, numbers, and the hyphen

Name	Description
	character (-). The first character cannot be a number.

Related topics:

[Setting up the Modular Messaging network](#) on page 41

Windows Domain field descriptions

Name	Description
Join a corporate windows domain?	Selection indicates that you want Modular Messaging to connect to the corporate Windows domain.
Join a private windows domain?	Selection indicates that you want Modular Messaging to join the private Windows domain.
Domain controller's host name (FQDN)	Specifies the host name of the domain controller of the corporate Windows domain that you want the Modular Messaging system to join.
Corporate Windows domain name	Specifies the name of the corporate Windows domain that you want the Modular Messaging system to join.
Windows domain name	(Optional) This name must be unique throughout the messaging network and should not be the same as the corporate Windows domain name.

Related topics:

[Setting up the Windows domain configuration](#) on page 42

Modular Messaging Configuration field descriptions

Name	Description
Mailbox number length	Specifies the number of digits that you want to have for your subscriber mailboxes.

Name	Description
Windows License Key	Specifies the product key for the copy of Windows that is installed on the MAS. The product key can be as many as 25 alphanumeric characters in groups of 5. Each 5 character group is separated with a hyphen -.
VMD name	Specifies the name of the voice mail domain. The VMD name can be from 2 to 16 characters, including any alphanumeric character and the characters: , _ % ^ & * () ~ @ and spaces.
Language used for both Announcement and TTS	The default language for announcements and TTS.
Web Client IP Address	(For Web Client only) Specifies the IP address of the Web Client server.
Web Client Name	(For Web Client only) Specifies the Fully Qualified Domain Name (FQDN) of the Web Client server. The FQDN (computer plus domain name) can be from 1 to 64 characters, including lower case alpha characters, numeric characters, and the hyphen -. The first character cannot be a number.
Windows License Key	(For Web Client only) Specifies the windows license key for the Web Client server.

Related topics:

[Configuring Modular Messaging](#) on page 43

Modular Messaging Accounts field descriptions

MM Accounts — MSS Account Information field descriptions

Name	Description
MSS Login 'sa' password	Specifies the local account password for MSS.
Confirm MSS Login 'sa' password	To confirm the local account password for MSS.
MSS Login 'vm' password	Specifies the virtual account password for MSS.

Name	Description
Confirm MSS Login 'vm' password	To confirm the virtual account password for MSS.
Trusted Servers Password	Specifies the password to log in to the trusted server.
Confirm Trusted Servers Password	To confirm the password to log in to the trusted server.

MM Accounts — MAS Logon Accounts and Passwords field descriptions

Name	Description
Technical Support logon name	Specifies the name of the logon account used by support personnel for remote system administration. The name can be from 4 to 32 characters. Do not include the abbreviation <i>craft</i> in the logon name.
Technical Support password	Specifies the password for the logon account used by support personnel for remote system administration. The password can be from 7 to 32 characters, including any alphanumeric character and the following characters: # % = + - _ () , . / ? @ [] { } and ~ . Avaya recommends that a password contain at least three of the following four entry classes: lowercase character, uppercase character, number, and punctuation mark or symbol.
Confirm Technical Support password	To confirm the password for the technical support user ID.
Customer account logon name	Specifies the name of the logon account used by the customer for system administration. The name can be from 4 to 32 characters. Do not include the abbreviation <i>cust</i> in the logon name.
Customer account logon password	Specifies the password for the logon account used by the customer for system administration. The password can be from 7 to 32 characters, including any alphanumeric character and the following characters: # % = + - _ () , . / ? @ [] { } and ~ . Avaya recommends that a password contain at least three of the following four entry classes: lowercase character, uppercase character, number, and punctuation mark or symbol.

Name	Description
Confirm Customer account logon password	To confirm the password for the customer account ID.

MM Accounts — MAS Admin Account field descriptions

Name	Description
MAS local administrator account logon	Specifies the name of the account used for local MAS administration. The name can be from 4 to 32 characters, including any alphanumeric character and the characters: . and _ . Do not include the abbreviation admin in the logon name.
MAS local administrator account password	Specifies the password to log on as a MAS local administrator. The password can be from 7 to 32 characters, including any alphanumeric character and the following characters: #%=+ -_ () , . / ? @ [] { } and ~ . Avaya recommends that a password contain at least three of the following four entry classes: lowercase character, uppercase character, number, and punctuation mark or symbol.
Confirm MAS local administrator account password	To confirm the password to log on as a MAS local administrator.

Related topics:

[Creating Modular Messaging accounts](#) on page 43

Switch Integration Information field descriptions

Name	Description
Switch Name	Specifies the name for SIP switch.
SIP Domain	Specifies a fully qualified domain name of the SIP domain.
SIP Gateway address	Specifies the IP address or fully qualified domain name of the SIP gateway.

Related topics:

[Configuring the switch integration](#) on page 44

Appendix C: Alternative methods for preparing the installation source

Setting up the HTTP server

Before you begin

- You must have the Modular Messaging template. For more information, see [Obtain a Modular Messaging template](#) on page 20.
- The HTTP server must be capable of transferring file sizes of up to 8Gb.

About this task

Perform the following tasks to copy the Modular Messaging template to an HTTP server that is accessible from the System Platform server.

Procedure

1. Create one of the following directories on an HTTP server:
 - **modular_messaging**: Modular Messaging without Web Client.
 - **wcwsso_mm**: Modular Messaging with Web Client.
2. Copy the optical media content on an HTTP server.
The following describes the file structure that should be maintained when you copy the optical media content to an HTTP server.

modular_messaging:

- mmpreconfig.war
- modular_messaging.mf
- modular_messaging.ovf
- mm_vm_images
 - mas_prepared_ver_11.1.gz
 - mss_prepared_ver_11.1.gz

wcwsso_mm:

- mmpreconfig.war
- modular_messaging.mf
- modular_messaging.ovf
- wcwso_mm.ovf
- wcwso_mm.mf
- mm_vm_images
 - mas_prepared_ver_11.1.gz
 - mss_prepared_ver_11.1.gz
 - wcwso_prepared_ver_11.2.gz

Setting up a USB flash drive

Before you begin

- You must have the Modular Messaging template. For more information, see [Obtain a Modular Messaging template](#) on page 20.
- You must use minimum 16GB USB flash drive.

About this task

You can copy the Modular Messaging template to the USB flash drive either from PLDS or optical media. Perform the following tasks to copy the Modular Messaging template from optical media to the USB flash drive.

Procedure

1. Connect the USB flash drive into USB port of a Linux based computer. Monitor what identification is used for the drive. You will require to use this identification while creating a Linux partition in the next step. Typically the identifier is *sdb*.
2. Type the following to create a Linux partition on the USB flash drive:
`fdisk /dev/sdb`. Where, *sdb* is the identifier.
When query selected
n - New Partition
p - Primary Partition
p if you want to view the properties you have selected
w to save
3. Type the following to format the USB flash drive:


```
mkfs -t ext3 /dev/sdb1
```

4. Type the following to mount the USB flash drive:

```
mount -t ext3 /dev/sdb1 /mnt
```

5. Insert the template CD into the CD-ROM of the System Platform.

- If you are installing Modular Messaging without Web Client, insert **Modular Messaging single server configuration Template MAS/MSS**
- If you are installing Modular Messaging without Web Client, insert **Modular Messaging single server configuration Template MAS/MSS/Web Client/WSO**

6. Type the following to mount the CD:

```
mount /dev/cdrom /media
```

7. Type the following to copy CD contents to the USB flash drive:

```
cp -r /media/modular_messaging /mnt
```

8. Type the following to unmount the CD:

```
umount /media
```

9. Insert other two disks (**Modular Messaging single server configuration Application - DVD 1 of 2** and **Modular Messaging single server configuration Application - DVD 2 of 2**) and repeat the steps 6 to 8.

10. Type the following to unmount the USB flash drive:

```
umount /mnt
```

Appendix D: Alternative methods of accessing the system

Accessing the MAS using the VNC viewer installed on the System Platform

If Remote Desktop is not available for the MAS, you can use VNC to gain access to the Windows console. The VNC connection will be made via the System Platform System Domain (Dom0) hence avoiding any networking issues.

Before you begin

- Ensure that you have Virtual Network Computing (VNC) viewer installed on your computer
- VNC server must be up and running on the System Platform

Procedure

1. Log in as `root` on `dom0`.
 2. Type the following command to start X Windows: `startx`
 3. Start VNC viewer and type the following to access the graphic console from the X terminal: `virt-viewer mas, ,` where `mas1` is host name of the MAS.
-

Accessing the MAS using the VNC viewer from a remote computer

If Remote Desktop is not available for the MAS, you can use VNC to gain access to the Windows console. The VNC connection will be made via the System Platform System Domain (Dom0) hence avoiding any networking issues.

Before you begin

- Ensure that you have Virtual Network Computing (VNC) viewer installed on your computer
- VNC server must be up and running on the System Platform

Procedure

1. Start an SSH session to Dom0.
 2. Find the VNC port of the MAS in one of the following ways:
 - Open the System Platform Web Console (`http://<ipaddress>/webconsole`). Navigate to **Virtual Machine Management > Manage > Virtual Machine List** to find the VNC port
 - In the command prompt, run the following command: `virsh vncdisplay mas1`, where `mas1` is host name of the MAS
 3. Use the following command in the command prompt to set up port forwarding for SSH:
`ssh -L 59<vnc_port_number>:localhost:59<vnc_port_number> admin@your_domain0_ip`
 4. Log in as the admin on dom0.
 5. Start the VNC viewer on your Personal Computer.
 6. Enter `localhost:59<vnc_port_number>` as the computer name, where `localhost` is the hostname of the computer that you want to access.
-

Accessing the MSS using PuTTY

Procedure

1. Start a PuTTY session.
 2. In the **Host Name**, enter the **IP address** of the MSS.
 3. Click **Open** to open a PuTTY session.
 4. Enter the login name in the **Login** field.
 5. Enter the password in the **Password** field.
-

Accessing the MSS using virsh console command through PuTTY

Procedure

1. Start a PuTTY session.
 2. In the **Host Name**, enter the **IP address** of the System Platform.
 3. Click **Open** to open a PuTTY session.
 4. Enter the login name in the **Login** field.
 5. Enter the password in the **Password** field.
 6. Type the following command after successful login: `su root`
 7. Enter the password for the *root* user.
 8. After gaining access to the root login of System Platform Web Console, type the following: `virsh console mss`
-

Alternative methods of accessing the system

Glossary

Active Directory	The directory service for a Microsoft Windows 2000, Windows 2003 Server, or Windows 2008 Server. The Active Directory stores information about objects on the network and makes this information available for authorized administrators and users. It provides administrators with an intuitive hierarchical view of the network and a single point of administration for all network objects.
Call Me	A feature that allows subscribers to be called at a designated telephone number or from a telephone list, each time they receive a message that meets specified criteria. The subscriber is then invited to log in to Avaya Modular Messaging to review their messages.
Caller Applications	Extensions to the Avaya Modular Messaging telephone user interface (TUI) used to customize how Avaya Modular Messaging interacts with callers.
Caller Applications Editor	An Avaya Modular Messaging tool that customizes the Microsoft Management Console (MMC) user interface to permit the creation, editing, and deployment of Caller Applications.
CCI	See CCS on page 0 .
CDOM	See Console Domain on page 0 .
Class of service	A category used to determine subscriber access to system options and features. The administrator assigns a COS to each subscriber.
Common Caller Interface (CCI)	An interface that allows callers to leave Call Answer messages. This interface is common to all callers irrespective of the TUI assigned to the called subscriber.
Console Domain	Console domain is a virtual machine, which is a part of System Platform and has many platform elements. <ul style="list-style-type: none">• Common logging and alarming• Remote access• System Platform Web Console• Upgrades and patches• WatchDog• Licensing

COS

COS

See [Class-of-Service](#) on page 0 .

Data Collection Tool (DCT)

The DCT has two primary uses. First, it is used to gather information that is required in order to install Modular Messaging. Second, it can collect information from an existing Modular Messaging system that can be used if the system has to be rebuilt after a catastrophic failure.

DCT

See [Data Collection Tool \(DCT\)](#) on page 0 .

DEM

See [Directory Enabled Management \(DEM\)](#) on page 0 .

DHCP

See [Dynamic Host Configuration Protocol \(DHCP\)](#) on page 0 .

Direct Inward Dialing

A DID extension can be dialed directly from the public telephone network, without going through a receptionist.

Digital Set Emulation (DSE)

Allows Modular Messaging to emulate a digital telephone in order to integrate digitally with some types of PBX. Also known as set emulation.

Directory Enabled Management (DEM)

An interface that uses Avaya Directory Server to facilitate administration of Modular Messaging (MSS) from a centralized location.

DSE

See [Digital Set Emulation \(DSE\)](#) on page 0 .

Dynamic Host Configuration Protocol (DHCP)

A protocol that dynamically assigns IP addresses to devices when they get connected to the network.

Find Me

A feature that allows a subscriber to configure a list of telephone numbers where they might be contacted, so that Modular Messaging can try to connect a caller to a subscriber before asking the caller to leave a message.

LDAP

See [Lightweight Directory Access Protocol \(LDAP\)](#) on page 0 .

Lightweight Directory Access Protocol (LDAP)

LDAP is an IP used to retrieve and manage directory information.

MAS

See [Messaging Application Server \(MAS\)](#) on page 0 .

Message Storage Server (MSS)

An Avaya-produced message store that is an integral part of the Modular Messaging system.

Messaging Application Server (MAS)

The voice server that provides an interface between the message store (and directory) and the telephone system.

Message Waiting Indicator (MWI)	A method of alerting subscribers when messages meeting specified criteria arrive in their mailboxes. Subscribers are alerted by either a lamp indicator on their telephone or an audible tone (stutter dialtone) when they pick up the receiver. The indicator is cleared when the message is opened in the e-mail client or saved or deleted using the TUI. Subscribers can set up rules for using MWI in Subscriber Options. For example, they may choose to be notified only when they receive urgent voice messages.
MWI	See Message Waiting Indicator (MWI) on page 0 .
Notify Me	With Notify Me, a subscriber gets notified when a message is received in their mailbox, or when a caller requests to notify them. The system can notify a subscriber by either sending an email message or by paging a numeric pager.
Notes client	Client software that provides access to Notes databases on a Domino server and allows them to send mail and browse the Web.
PDL	See Personal Distribution List (PDL) on page 0 .
Password	<p>A number required by subscribers to gain access to Modular Messaging through different interfaces, such as the TUI, desktop computer interfaces, and the one-X Speech client. Subscribers can change their passwords by using the TUI or Subscriber Options.</p> <p>A number required by subscribers to gain access to Messaging through different interfaces, such as the TUI, desktop computer interfaces, and the one-X Speech client. Subscribers can change their passwords by using the TUI.</p>
PBX	See Private Branch Exchange (PBX) on page 0 . Synonymous with switch.
PBX Integration	A method that establishes communication between the PBX and the voice mail system. The PBX supplies information, such as the identity of the caller who is calling on internal calls and the extension that the caller is trying to reach. Also known as switch integration.
Personal Distribution List (PDL)	A labeled collection of addresses that subscribers create and save for use later. Messages that subscribers address to the list are sent to all the multiple addresses (list members) within the list. Subscribers can manage and address messages to only those PDLs that they create and own.
PLDS	The Avaya Product Licensing and Delivery System (PLDS) provides easy-to-use tools for managing asset entitlements and electronic delivery of software and related licenses. Using PLDS, you can perform

activities such as license activation, license deactivation, license re-host, and software downloads.

Port Monitor

A diagnostic tool that provides a graphical user interface (GUI) for checking and changing the status of ports on a particular MAS.

Private Branch Exchange (PBX)

A telephone exchange local to a particular organization, having a switchboard and associated equipment. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX. Also known as a switch.

Public Switched Telephone Network

A common carrier network that provides circuit switching between public users.

SAL Gateway

A customer-installable system that provides remote access, and alarming capabilities for remotely managed devices.

Secure Access Link (SAL)

SAL is an Avaya serviceability solution for support and remote management of a variety of devices and products. SAL provides remote access and alarm reception capabilities. SAL uses the existing Internet connectivity of a customer to facilitate remote support from Avaya.

Secure Sockets Layer (SSL)

A protocol for transmitting private documents or messages through the Internet.

Session Initiation Protocol (SIP)

A signaling protocol that allows exchange of information, such as call information, signaling information, and voice data using voice channels over an IP network.

Simple Mail Transfer Protocol (SMTP)

A TCP/IP protocol used for sending and receiving e-mail. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another and to send messages from an e-mail client to an e-mail server.

Simplified Message Desk Interface (SMDI)

A protocol that is used for sending switch integration data. This protocol does not require a caller to re-enter the telephone number if the extension is busy or not answered.

Simple Network Management Protocol (SNMP)

A protocol for managing and monitoring networks.

SIP

See [Session Initiation Protocol \(SIP\)](#) on page 0 .

SIP Gateway

The SIP gateway allows a Modular Messaging system to work with PBXs that are not supported by the SES, mainly those from third-party vendors.

The SIP gateway allows a Messaging system to work with PBXs that are not supported by the SES, mainly those from third-party vendors.

SMTP	See Simple Mail Transfer Protocol (SMTP) on page 0 .
SNMP	See Simple Network Management Protocol on page 0 .
SPIRIT	Beginning with Modular Messaging Release 4.0, all systems are installed with SPIRIT, which provides remote serviceability using IP access. SPIRIT replaces the older modem-access agents, including Avaya Serviceability Agent.
SSL	See Secure Sockets Layer (SSL) on page 0 .
Subscriber	A user whose profile is enabled for voice messaging. A subscriber can use both the TUI and the GUI of Modular Messaging.
Subscriber Options	An application that allows subscribers to configure their mailboxes by using their computers. Subscribers can record all personal greetings and prompts, personalize their call handling options, and select whether to use multimedia or telephone for recording and playing back voice messages.
Switch	Synonymous with PBX.
Telephone user interface (TUI)	An interface through which callers and subscribers can gain access to the Modular MessagingMessaging system by means of the telephone. The TUI is an Automated Attendant and voice-messaging system that controls call handling. It greets incoming callers and instructs them on how to proceed.
Text-to-speech (TTS)	The conversion of text into speech (speech synthesis). Using TTS, Modular MessagingMessaging subscribers can listen to the envelope information of messages, text names, and e-mail messages over the telephone.
TTS	See Text-to-speech (TTS) on page 0 .
TUI	See Telephone user interface (TUI) on page 0 .
VMD	See Voice Mail Domain (VMD) on page 0 .
VMSC	See Voice Mail System Configuration (VMSC) .
Voice Mail Domain (VMD)	A group of MAS units that share a common set of properties. All subscribers who are provided with telephone answering by these MAS units belong to the same VMD.
WebLM	WebLM is a Web-based licensing solution that facilitates license management. It is part of the Avaya Integrated Management System

Manager. Using WebLM, an administrator can track and manage licenses of multiple Avaya software products installed in an organization from a single location. WebLM requires a license file that contains information about the product, including the major release, the licensed features of the product, and the licensed capacities of each feature bought by your organization.

Index

A

acceptance testing	69
access	33
accessibility	12
accessing	34–36 , 123–125
console domain	34
MAS	35 , 123 , 124
MSS	35 , 124 , 125
putty	124 , 125
RDC	35 , 36
remote computer	124
system domain	34
system platform	123
virsh console command	125
VNC	123 , 124
web client	36
web console	35
account	43 , 116
Modular Messaging	43 , 116
activating	48
Microsoft Windows	48
adding	30 , 47
MSS	47
trusted site	47
adding test subscribers	69
administrator accounts	43 , 116
alarming	12 , 82
analyze current configuration	88
anti-virus software	50
install, administer	50
applying	52
applying licenses	52

B

back up	93
backin up	93

C

call answer message	71
leaving	71
caller applications	103
checking	89
checklist	14

installation	14
complete	100
completing	100
computer accounts	26
configuration	45
save	45
configure	22 , 23 , 43 , 115
Modular Messaging	43 , 115
configure network	22
configuring	22 , 44 , 81 , 83
MAS	83
serviceability settings	83
switch	44
system alarms	81
configuring Call Me service	55
configuring languages and multi-lingual TTS	61
configuring MM Audit Service	56
configuring MWI service	55
configuring Notify Me	55
configuring offline access to messages	62
configuring specific features as needed	54
copy	64
software updates	64
copying template	24
corporate network	41 , 113
corporate windows domain requirements	25
creating	26 , 77
fax messages	77
creating and sending	74
messages in in non-integrated mode	74

D

date and time	22
Dialing rule	61
DNS	41 , 113
domain	42 , 115
Windows	42 , 115
domain name servers	113
Domain Name Servers	41
download	63
software updates	63

E

entering	54
----------------	--------------------

MAS	54	updates	65 , 66
product id	54	message	71 , 72
<hr/>			
F		call answer	71
fax message	77	test	72
create	77	messages in non-integrated mode	74
print	77	sending	74
Fax Service Manager	60	creating	74
<hr/>			
H		Microsoft Windows	48 , 49
HP DL360 G7	17	activate	48
baseline specifications, configuration, and options	17	internet activation	48
HTTP server	119	telephone activation	49
<hr/>			
I		MM Fax Printer	59
importing certificates	52	MM Fax Sender server	57
install	65–67	MM Fax Sender server in VMSC	57
MAS updates	65	Modular Messaging ...	37 , 39 , 40 , 42–44 , 63 , 114–116 , 118
software updates	66 , 67	accounts	43 , 116
install system platform	21	configure	43 , 115
installation	14 , 46	local accounts	43 , 116
checklist	14	network	42 , 114
installation worksheet	109	software update	63
installing and administering anti-virus software	50	update	63
integrated mode	72	switch	44 , 118
test message	72	template	37 , 39 , 40
integration	44 , 118	Modular Messaging network	42 , 114
switch	44 , 118	set up	42 , 114
<hr/>			
L		Modular Messaging template	37 , 39 , 40
legal notices	2	configuration	40
license	12 , 50	customizing	39
license requirements	12	installing	37
licenses	51 , 52	MSS	66 , 79 , 82 , 87 , 93 , 95 , 96
location	39	backup	87
selecting	39	recover	95
<hr/>			
M		software updates	66
managed devices	30	test subscribers	79
managing license	50	MSS administration	100
MAS	64–66 , 87 , 89 , 93 , 95	<hr/>	
backup	87 , 89	N	
recoveing	95	network	41 , 42 , 113 , 114
recover	95	Modular Messaging	42 , 114
running backup	87 , 89	set up	41 , 113
<hr/>			
O		new Installation	69
obtain licenses	51	acceptance testing	69
obtain template	20	notices, legal	2
obtaining	51	<hr/>	
One-way trust	58	O	

outcalling capability	75
test	75

P

PBX	23
PLDS	24
preparing for installation	24
prerequisite	17
printing	77
fax messages	77

R

recover	95
MAS	95
MSS	95
registering	24 , 29
system	29
remote	12
remove	79
test subscribers on MSS	79
restarting the messaging services	98
restore	96 , 103
restore data	96
restoring	86 , 103
MAS	86
snapshot	86
retrieve	72
test messages	72
run	87 , 89
backup	87
backup on MAS	89
backup on MSS	87
running	95
MSS restore	95

S

S8800 1U Server	17
SAL	22
saving	45
configuration	45
security	13
security considerations	13
sending	74
messages in non-integrated mode	74
setting	119 , 120
setting up	41 , 42 , 113–115 , 118
Modular Messaging network	42 , 114
network	41 , 113

switch	118
Windows	42 , 115
setup	82
software update	63
Modular Messaging	63
software updates	63 , 64 , 66 , 67
download	63
installing	66 , 67
MSS	66
web client	67
SP server	24
specifying	82
alarm	82
MSS	82
spool folder	89
switch	44 , 118
integration	44 , 118
system	33
system platform	10
system specifications	17

T

taking	85
MAS	85
snapshot	85
Telephone activation	49
Microsoft Windows	49
template	37–40
locating	38
Modular Messaging	37 , 39 , 40
test	75
outcalling capability	75
test message	72
retrieve	72
test Subscriber	79
MSS	79
test subscribers on MSS	79
removing	79
testing	69 , 83
acceptance	69
new installation	69
alarming	83
origination	83
troubleshooting	105–107
configuration problem	105
insufficient resources	105
MSS configuration failed	106
successful configuration	107
System Platform Management Console	107
template install log	106

U

update	63
Modular Messaging	63
updates	65 , 66
MAS	65 , 66
updating Microsoft windows	49
USB flash drive	120
user accounts	26
using DCT	88

V

verify	46 , 53 , 66
MAS updates	66

WebLM URL in VMSC	53
verifying	46
VMSC setup	100

W

web client	67
software updates	67
WebLM URL in VMSC	53
verifying	53
Windows	42 , 48 , 115
domain	42 , 115
internet activation	48
set up	42 , 115