

Modular Messaging for Microsoft Exchange

Release 5.2

Installation and Upgrades

February 2012
Issue 1.4

© 2012 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site:

http://www.avaya.com/support

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

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 Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s)

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use 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 identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

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 might 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 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://www.avaya.com/support

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that can be accessed by this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who might be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions might be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there might be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it might result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you — Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers might experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment is the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. might void the user's authority to operate this equipment.

Federal Communications Commission Statement

Part 15:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

European Union Declarations of Conformity



Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the Avaya Support Web site:

http://www.avaya.com/support

Trademarks

Avaya and the Avaya logo, Aria, AUDIX, DEFINITY, INTUITY, Serenade, Mailbox Manager and COMPAS are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

COMPAS

This document is also available from the COMPAS database. The COMPAS ID for this document is 149235.

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 Support Web site:

http://www.avaya.com/support

Contents

About this book xiii
Intended audience xiii
Changes to this book xiv
How to use this book xiv
Installing a new system xv
Upgrading, migrating, or recovering a system xv
Using links in this document xvi
Trademarks xvii
Related resources xvii
User documentation xvii
Technical assistance xvii
Remote support center xvii
Help on the system xviii
Training xviii
How to comment on this book xviii

Chapter 1: Preinstallation requirements 1
Software shipped with the system 2
Obtaining the DCT data file 3
Downloading required software and documentation 3
Downloading software updates 4
Downloading configuration notes 4
Downloading the installation and upgrade checklists 5
Downloading user documentation 5
Security considerations 6
On-site security considerations 6
Password security 6
System security during installation 6
Ongoing system security considerations 7
Test equipment recommendations 7
Initial switch and LAN administration 8
Initial switch or PBX administration 8
Initial LAN administration 8

Chapter 2: Preparing to install Modular Messaging software 9
Overview 9
Setting up Modular Messaging accounts 10
Creating Modular Messaging customer and technical support accounts . . . 10
Creating the Modular Messaging customer account 11
Creating the Modular Messaging technical support account 13

Creating test subscriber accounts 14
Using Power Shell to create a Modular Messaging service permissions group . 16
Assigning permissions to the Modular Messaging service permissions group . 17
Assigning Send As permission 17
Assigning additional permissions 19
Assigning permissions with Exchange 2010 19
Assigning permissions with Exchange 2007 22
Assigning permissions with Exchange 2003 24
Preparing Exchange 2010 27
Creating MAS computer accounts 31
Setting up each server for remote access 32
Updating the Active Directory schema 33
Logging on and preparing to update 33
Adding the Schema Update registry key 34
Running the Modular Messaging installation wizard 34
Updating the Active Directory 35
Configure NSPI for Windows Server 2008 domain controllers: 36

Chapter 3: Adding Exchange extensions for Modular Messaging 37
Overview 38
Adding the Exchange extensions 40
Logging on and preparing to update 40
Running the Modular Messaging installation wizard 41
Adding the Exchange extensions 41
Adding the Exchange extensions after installing the Modular Messaging software 43

Chapter 4: Configuring an Avaya MAS 45
Completing MAS configuration prerequisites 46
Displaying an MAS from the console. 48
Configuring MASs using an existing DCT data file 49
Installing third-party software 51
Updating Windows Internet Explorer 7 security 51
Installing third-party software for Exchange 2010 52
Installing third-party software for Exchange 2007 52
Installing third-party software for Exchange 2003 53
Completing the MMCW configuration 53
Completing the MAS configuration 54
Administering antivirus software 54
Installing software updates 55
Disabling the private LAN 55

Entering RAS IP addresses on each MAS 56
Continuing the installation 57

Chapter 5: Configuring a customer-provided MAS 59
Customer-provided MAS configuration prerequisites 60
Preparing the customer-provided MAS 61
Installing Microsoft Windows 2003 R2 operating system 62
Setting a computer name 62
Running recommended disk checks 62
Installing modem drivers on the customer-provided MAS 62
Adjusting system values 62
Installing and enabling Microsoft Windows services 64
Installing Microsoft Windows 2003 SP2 66
Installing Microsoft Windows updates and security patches 66
Joining the Windows domain 67
Adding Modular Messaging accounts to the local administrators group . . . 68
Configuring the customer-provided MAS 68
Running the Modular Messaging Configuration wizard 69
Installing third-party software 71
Updating Windows Internet Explorer 7 security 72
Installing third-party software for Exchange 2010 72
Installing third-party software for Exchange 2007 73
Installing third-party software for Exchange 2003 73
Completing the MMCW configuration 74
Completing the customer-provided MAS configuration 74
Installing software updates 75
Verifying default LAN name and Power Management settings 75
Entering the RAS IP addresses on customer-provided MAS 76
Setting logging location 77
Continuing the installation 78

Chapter 6: Configuring the voice mail system 79
Configuring the voice mail system 79
Configuring required domain-wide features 80
Specifying languages 81
Verifying that Modular Messaging service has started on MAS#1 81
Configuring TUI and access settings 82
Configuring the broadcast mailbox 83
Configuring the PBX type 86
Configuring serviceability settings 86
Installing and configuring the WebLM server on an MAS 89

Installing WebLM server on an MAS 90
Obtaining the license file 91
Applying license file on the WebLM server 91
Importing certificates from license 92
Configuring the WebLM URL in VMSC 92
Entering Product ID for current MAS 93
Configuring specific features as needed 93
Configuring Call Me service 94
Configuring Notify Me 94
Configuring MWI service 95
Configuring languages and multi-lingual TTS 95
Configuring Audit Service 96
Configuring the MM Fax Sender server 96
Configuring offline access to messages 98
Configuring MAS-specific parameters 99
Configuring INADS alarming, if used 99
Configuring port boards and switch integration 100
Restarting messaging services 102
Verifying basic operation of this MAS 104
Verifying call-handling capability 104
Verifying alarming setup 104
Verifying Tracing Service operation 105
Verifying Audit Service 106
Continuing the installation 106

Chapter 7: Testing and backing up the system 107
Adding a test subscriber 108
Setting up monitoring tools—optional 110
Using the Operational History Viewer 110
Setting up the port monitor 111
Performing acceptance tests 112
Creating and sending a call-answer message 112
Retrieving test messages in integrated mode 112
Creating and sending a test message in nonintegrated mode 114
Testing the outcalling capability 115
Creating and printing a fax message 117
Running additional tests 118
Removing the test subscribers 118
Backing up the system 119
Running periodic checks 120

Turning over the system to the customer 120

Chapter 8: Upgrading Modular Messaging software on an Avaya MAS 123
Upgrading from Release 5.1 to Release 5.2 124
Upgrading from Release 3.x or Release 4.0 to Release 5.2 125
Upgrade requirements. 125
Preparing for the upgrade from Release 3.x or 4.0 126
Considerations for multiple-MAS upgrades 127
Switching the monitor to show the correct server 127
Performing pre-upgrade tasks 128
Verifying and saving data 128
Using the DCT to collect information from an MAS 130
Busying out ports 132
Backing up the MAS 132
Running recommended disk checks 133
Logging off all remote logins 133
Stopping Modular Messaging services. 133
Applying Microsoft Windows Server 2003 Service Pack 2 133
Updating Windows Internet Explorer 7 security 134
Upgrading Modular Messaging software. 134
Upgrading Overnight 135
Upgrading RealSpeak software 135
Starting all Modular Messaging services. 136
Upgrading Dialogic drivers 136
Upgrading MAS software 137
Completing server setup 139
Verifying antivirus software 139
Installing and configuring WebLM server 139
Installing software updates 140
Updating Microsoft Windows 140
Enabling ports 140
Completing the Release 3.x or 4.0 to Release 5.2 upgrade 141

Chapter 9: Upgrading Modular Messaging software on a customer-provided server 145
Upgrading from Release 5.1 to Release 5.2 146
Upgrade requirements. 147
Preparing for the upgrade from Release 3.x or 4.0 149
Considerations for multiple-MAS upgrades 150
Switching the monitor to show the correct server 150
Performing pre-upgrade tasks 150

Verifying and saving data . . . 151
Using the DCT to collect information from an MAS . . . 152
Busying out ports . . . 154
Backing up the MAS . . . 155
Running recommended disk checks . . . 155
Logging off all remote logins . . . 155
Stopping Modular Messaging services . . . 156
Installing Microsoft Windows prerequisite components . . . 156
Applying Microsoft Windows Server 2003 Service Pack 2 . . . 156
Updating Windows Internet Explorer 7 security . . . 157
Upgrading Modular Messaging software . . . 158
Upgrading Overnight . . . 158
Upgrading RealSpeak software . . . 158
Starting all Modular Messaging services . . . 159
Upgrading Dialogic drivers . . . 159
Upgrading MAS software . . . 161
Completing server setup . . . 163
Verifying antivirus software . . . 163
Installing software updates . . . 163
Updating Microsoft Windows . . . 164
Enabling ports . . . 164
Completing the Release 3.x or 4.0 to Release 5.2 upgrade . . . 165

Chapter 10: Migrating to Modular Messaging Release 5.2 on an Avaya MAS . . . 169
Migration requirements . . . 169
Preparing for the migration . . . 172
Considerations for multiple-MAS migration . . . 173
Changing Switch Integration . . . 174
Changing from Analog, DSE, or QSIG to SIP . . . 174
Changing from H.323 to SIP . . . 175
Analyzing the existing system . . . 176
Verifying and saving data . . . 176
Backing up the MAS . . . 177
Configuring the new S8800 1U server . . . 178
Adding the new S8800 1U server . . . 178
Installing third-party software . . . 181
Updating Windows Internet Explorer 7 security . . . 181
Installing third-party software for Exchange 2010 . . . 182
Installing third-party software for Exchange 2007 . . . 182
Installing third-party software for Exchange 2003 . . . 183

Completing the MMCW configuration 183
Completing the server setup 185
Installing and configuring WebLM server 185
Installing software updates 185
Updating Microsoft Windows 186
Disabling the private LAN 186
Entering RAS IP addresses on each MAS 186
Disabling the Avaya S3400, S3500, or S8730 servers 189
Busying out ports 189
Logging off all remote logins 189
Disabling services 190
Completing the migration 190
Reducing the number of servers 191

Chapter 11: Migrating to Modular Messaging Release 5.2 on a customer-provided server193
Migration requirements 194
Preparing for the migration 195
Considerations for multiple-MAS migration 196
Preparing the customer-provided server 197
Installing Microsoft Windows 2003 R2 operating system 197
Installing and enabling Microsoft Windows services 197
Setting a computer name 199
Installing Microsoft Windows 2003 SP2 199
Configuring the network card 200
Running recommended disk checks 200
Installing modem drivers on the customer-provided MAS 200
Setting up the new server for Modular Messaging 201
Joining the Windows domain 201
Adjusting system values 202
Adding Modular Messaging accounts to the local Administrators group 204
Changing Switch Integration 205
Changing from Analog, DSE, or QSIG to SIP 205
Changing from H.323 to SIP 206
Analyzing the existing system 206
Verifying and saving data 206
Backing up the MAS 207
Installing and Running the Modular Messaging Configuration wizard 208
Running the Modular Messaging Configuration wizard 208
Installing third-party software 212

Updating Windows Internet Explorer 7 security 212
Installing third-party software for Exchange 2010 213
Installing third-party software for Exchange 2007 213
Installing third-party software for Exchange 2003 214
Completing the MMCW configuration 214
Completing the server setup 216
Installing and configuring WebLM server 216
Installing software updates 216
Updating Microsoft Windows 217
Verifying default LAN name and Power Management settings 217
Entering RAS IP address on each MAS 218
Setting logging location 219
Disabling the customer-provided server 221
Busying out ports 221
Logging off all remote logins 221
Disabling services 222
Completing the migration 223

Appendix A: Installation, upgrade, and migration checklists 225
New Modular Messaging installation on an Avaya MAS 226
New Modular Messaging installation on a customer-provided MAS 230
Modular Messaging upgrade on an Avaya MAS 236
Modular Messaging upgrade on a customer-provided MAS 241
Modular Messaging migration on an Avaya MAS 245
Modular Messaging migration on a customer-provided MAS 249

Appendix B: Post-installation procedures for Modular Messaging 253
Updating client software 254
Disabling Modular Messaging services you plan to move 255
Moving Modular Messaging services among servers 257
Moving Call Me, MWI, and Mailbox Monitor 257
Updating the Call Me Server 257
Updating the MWI Server 258
Updating the MAS port groups 258
Moving MM Fax Sender service 259
Moving Audit service 261
Moving Tracing Server service 261
Enabling the services on the correct server 263
Stopping all Modular Messaging services 263
Enabling the appropriate services 263

Restarting messaging service . . . 265
Completing the move services procedure . . . 266
Converting Supplementary server to run a 0 port MAS on the Supplementary server 267
Changing switch integration . . . 269
Changing from DSE or Analog to QSIG . . . 269
Changing from DSE or QSIG to H.323 . . . 270
Changing from DSE or QSIG to SIP . . . 272
Changing from QSIG T1 to QSIG E1 . . . 273
Changing from H.323 to SIP . . . 274

Appendix C: Creating a new tone file . . . 277
Learning tones automatically . . . 278
Running the PBXpert wizard . . . 278
Consolidating and saving the TSF file . . . 280
Using the new TSF in Dialogic Configuration Manager . . . 280
Learning tones manually . . . 281
Running PBXpert . . . 281
Adding a new tone set . . . 282
Learning tone definitions . . . 282
Testing the tone set . . . 283
Consolidating and saving the TSF file . . . 283
Using the new TSF in Dialogic Configuration Manager . . . 284

Appendix D: Installing Dialogic port boards in a customer-provided MAS . . . 285
Supported MAS port boards . . . 286
Installing MAS port boards . . . 287
Preparing for the installation . . . 287
Setting jumpers and switches . . . 288
D/480JCT-1T1 and D/600JCT-1E1 or D/600JCT-2E1 QSIG board settings . . . 289
D/480JCT-1T1-EW and D/600JCT-E1-120-EW QSIG board settings . . . 289
D/82JCT-U PCI Univ set emulation board settings . . . 290
D/82JCT-U EW set emulation board settings . . . 291
D/120JCT-LS 12-port analog board settings . . . 292
D/120JCT-LS-EW port analog board settings . . . 292
D/41JCT-LS 4-port analog board settings . . . 294
D/41JCT-LS-EW analog board settings . . . 295
Installing the port boards . . . 298
Disabling the Dialogic hardware . . . 299
Connecting MAS port boards to the switch . . . 300
Completing the hardware installation . . . 301

Appendix E: Updating Modular Messaging software 303
Obtaining software updates from the Web 303
Installing software updates on each MAS 304
Copying files to the MAS 304
Installing the updates on each MAS 305

Appendix F: Configuring and testing port boards 307
Overview 307
When to configure port boards 307
Supported port boards 308
Configuring port boards. 309
Configuring T1-QSIG or E1-QSIG boards 310
Configuring set emulation boards 312
Configuring analog port boards 314
Testing the port boards 317
Preparing for the test 317
Testing the ports 318

Appendix G: Reloading software on an Avaya MAS 321
Loading new MAS software 321
Loading the new software 322
Preparing the server to boot 323
Activating Microsoft Windows 324
Activating Microsoft Windows using a telephone 324
Activating Microsoft Windows through the Internet. 325

Appendix H: Removing Modular Messaging components from an MAS 327
Removing software components 328

Appendix I: Catastrophic Disk failure recovery 329
Recovering from a catastrophic disk failure on an Avaya MAS 330
Overview 330
Requirements for restore of Avaya MAS 330
Restoring the Avaya MAS 332
Recovering from a catastrophic disk failure on a customer-provided MAS 336
Overview 336
Requirements for restore of customer-provided MAS 336
Restoring the customer-provided MAS 338

Appendix J: Installing and configuring the AudioCodes gateway 343
Installation prerequisites 344

Installing and configuring the AudioCodes gateway at switch location 345
Continue configuring the AudioCodes gateway 348

Appendix K: Administrator reference 351
Exchange 2003, 2007, and 2010 group permissions 351
Send As permission 354
Active Directory schema updates 355

Appendix L: Migrating Modular Messaging to Exchange 2007 357
Installing Modular Messaging with Exchange 2007 358
Installation requirements 358
What's new with Exchange 2007 358
Installing Modular Messaging with a separate Exchange 2007 VMD 360
Installation requirements 360
What's new with Exchange 2007 361
Continuing the installation 361
Moving mailboxes to a new Exchange 2007 VMD 362
Migrating Modular Messaging to Exchange 2007 363
Installation requirements 363
What's new with Exchange 2007 364
Continuing the installation 364
Moving mailboxes to the Exchange 2007 server 365
Assigning MASs to Exchange 2007 peer mail server 366
Required software 366
Installing Exchange 2007 Management Tools 366
Changing to the Exchange 2007 peer mail server 368
Creating the non-peer Exchange 2003 monitor mailbox 369

Appendix M: Migrating Modular Messaging to Exchange 2010 371
Migrating Modular Messaging to Exchange 2010 372
Installation prerequisites 372
Changing the monitor mode 372
Removing the fail over peers 373
Preparing Exchange 2010 374
Migrating the Peer Exchange server to Exchange 2010 377
Preparation 378
Changing the Peer Exchange server for a MAS 378
MAPI/CDO installation 379
Migrating from Exchange 2003 to Exchange 2010 379
Migrating from Exchange 2007 to Exchange 2010 380

Reassigning the Peer Exchange server for a MAS 380
Relocating the VMD mailbox 381
Clean up the system mailboxes 382
Removing the Peer Exchange system mailbox 382
Continuing with the migration 383
Creating the non-peer Exchange 2003 system mailbox. 383
Moving the Fax system mailbox 384
Moving Subscriber Mailboxes to Exchange 2010 384
Finishing off 385

Appendix N: Diminished Permissions for Microsoft Exchange 2003 and Exchange 2007387
Overview 387
Setting up Modular Messaging accounts 388
Creating Modular Messaging customer and technical support accounts . . . 389
Creating the Modular Messaging customer account 389
Creating the Modular Messaging technical support account. 391
Creating test subscriber accounts 392
Assigning permissions to the customer account group 392
Manually create the VMD container 396
Assigning permissions to the root of the Forest 397
Changing the permissions of the Deleted Objects container. 398
Allowing Send As permissions to protected groups 400
Creating MAS computer accounts 402
Updating the Active Directory and data schema 403
Logging on and preparing to update 403
Enabling Schema Updates by means of the Registry 403
Updating the Active Directory for Modular Messaging 404
Running the Modular Messaging installation wizard 404
Updating the Active Directory 405

Index 407

About this book

This book, *Avaya Modular Messaging for Microsoft Exchange Release 5.2 Installation and Upgrades* contains instructions for installing, upgrading, and migrating the Avaya Modular Messaging software in a Microsoft Exchange environment.

The Avaya-provided hardware for Modular Messaging Release 5.2 is Avaya S8800 1U server. Modular Messaging Release 3.0, Release 3.1, Release 4.0, or Release 5.1 on Avaya S3500 servers or Avaya S8730 servers can be upgraded to Release 5.2 or migrated to the S8800 1U servers.

Note:

Avaya does not support Avaya S3400 server in Release 5.2. However, this book provides instructions to migrate to an S8800 1U server.

Customer-provided equipment (CPE) for a Modular Messaging installation, upgrade, or migration must match the specifications described in *Avaya Modular Messaging Concepts and Planning Guide*.

Information in this book includes:

- Instructions to implement Modular Messaging with Exchange 2010, Exchange 2007, and Exchange 2003.
- Instructions to install, configure, administer, and acceptance test a new Modular Messaging for the Microsoft Exchange system.
- Instructions to upgrade the software from a Modular Messaging Release 3.x, Release 4.0, or Release 5.1 system to Release 5.2.
- Instructions to migrate Modular Messaging system Release 3.x, Release 4.0, or Release 5.1 from an Avaya S3400 server, an S3500 server, or an S8730 server to Release 5.2 on an S8800 1U server.

Intended audience

The book will be useful to designated experts who are responsible for:

- Installation and configuration of software on the Avaya S8800 1U servers and customer-provided servers.
- Upgrade from Release 3.x, Release 4.0, or Release 5.1 system that runs on an S3500 server, an S8730 server, or a customer-provided server to Modular Messaging Release 5.2.
- Migration from Release 3.x, Release 4.0, or Release 5.1 running on an S3400, S3500, or S8730 server to Modular Messaging Release 5.2 on an S8800 1U server.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.

- Migration from Release 3.x, Release 4.0, or Release 5.1 running on a customer-provided server to Modular Messaging Release 5.2.

Users of this book must be familiar with administering Microsoft Windows 2003 server or Microsoft Windows 2008 server, and Microsoft Exchange 2003, 2007, or 2010. Avaya assumes that users have read the *Avaya Modular Messaging Concepts and Planning Guide*.

Technicians who install an Avaya-provided Messaging Application Server should have completed a relevant hardware installation training course. For information on training, see Related resources on page xvii.

Changes to this book

Changes to this book include:

- New procedures to obtain, install, and configure the Modular Messaging license managed by Avaya Web License Manager (WebLM).
- Procedures to install and migrate to Release 5.2 to reflect support for the SAL only for alarming and remote access. However, this book still contains references to alarming and remote access other than SAL. Use these procedures only when you are upgrading Modular Messaging to Release 5.2.
- Procedures to install and migrate to Release 5.2 to reflect support for the SIP based switch integration only. However, this book still contains references to legacy port boards and H.323 integrations. Use these procedures only when you are upgrading Modular Messaging to Release 5.2.
- Release 5.2 software installation, upgrade, and migration procedures for the Avaya and customer-provided servers.

  Note:

  This document provides the information ***only*** on software installation, upgrades, and migration of the Avaya Modular Messaging system in a Microsoft Exchange server configuration. See *Installing the Avaya S8800 Server for Modular Messaging* guide for more information about installing the new hardware. For instructions to download the documents, see Downloading required software and documentation on page 3.

How to use this book

Review the appropriate section, depending on whether you are installing a new Avaya Modular Messaging system, or upgrading, or migrating a Modular Messaging system that is already in service.

Installing a new system

This document describes how to install Avaya Modular Messaging software either on a customer-provided Messaging Application Server (MAS), or on hardware provided by Avaya. Avaya-provided hardware is called the *Avaya MAS* in this guide. Although most steps are similar for both types of installation, this guide contains sections that are applicable only to one or another of these specific hardware types, as noted in the text.

Before you start a new installation:

1. Verify that the hardware meets the requirements specified in the *Avaya Modular Messaging Concepts and Planning Guide*. The planning guide explains important concepts and provides information that is crucial for planning a Modular Messaging installation.
2. The project planner, system administrator and other designated experts create a Data Collection Tool (DCT) data file prior to the installation. Send this file to the on-site technical support representative.
3. Print the checklist for a new installation from Appendix A: Installation, upgrade, and migration checklists on page 225. Use it to track your progress. There are different checklists for the Avaya MAS and customer-provided MAS. Be sure to print the checklist for your configuration.
4. Read Chapter 1: Preinstallation requirements on page 1. This chapter lists installation prerequisites, including the required documentation, software, tools, and equipment that you need to complete an installation.

Using the checklist as a guide, follow the directions in each subsequent chapter to install, configure, and test the Modular Messaging software.

Upgrading, migrating, or recovering a system

To upgrade a Modular Messaging system from either an Avaya MAS or a customer-provided MAS:

1. Obtain the following before you start the upgrade:
   a. Planning forms for the system that runs Release 3.x and the original DCT file for the system that runs on Release 4.0 or Release 5.1
   b. The latest analyzed DCT file for the system.
2. Print the relevant upgrade checklist from Appendix A: Installation, upgrade, and migration checklists on page 225. Use it to track your progress. Be sure to print the checklist for your configuration.
3. Obtain the software and documentation listed in the chapter overview for the configuration you are upgrading.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.

To upgrade a Modular Messaging system for either the Avaya MAS or customer-provided MAS:

- Follow the instructions in Chapter 8: Upgrading Modular Messaging software on an Avaya MAS on page 123.
- Follow the instructions in Chapter 9: Upgrading Modular Messaging software on a customer-provided server on page 145.

To migrate a Modular Messaging system from either an Avaya MAS or customer-provided MAS:

1. Obtain the following before you start the upgrade:
   a. Planning forms for a system that runs Release 3.x or the original DCT file for the system that runs Release 4.0 or Release 5.1
   b. The latest analyzed DCT file for the system.
2. Print the relevant migration checklist from Appendix A: Installation, upgrade, and migration checklists on page 225. Be sure to print the checklist for your configuration.
3. Follow these migrations instructions:
   - For migration of Avaya MAS, see Chapter 10: Migrating to Modular Messaging Release 5.2 on an Avaya MAS on page 169.
   - For migration of customer-provided MAS, see Chapter 11: Migrating to Modular Messaging Release 5.2 on a customer-provided server on page 193.

To migrate a Modular Messaging system to Exchange 2007 or Exchange 2010, follow these migrations instructions:

- For migration to Exchange 2007, see Appendix L: Migrating Modular Messaging to Exchange 2007 on page 357.
- For migration to Exchange 2010, see Appendix M: Migrating Modular Messaging to Exchange 2010 on page 371.

To recover an MAS from a catastrophic disk failure:

1. You must have the latest analysed DCT file. For Release 3.x, get the latest planning form.
2. Follow the procedures in Appendix I: Catastrophic Disk failure recovery on page 329 to recover a MAS:
   - For an Avaya MAS, follow the procedures mentioned in Recovering from a catastrophic disk failure on an Avaya MAS on page 330.
   - For a customer-provided MAS, follow the procedures mentioned in Recovering from a catastrophic disk failure on a customer-provided MAS on page 336.

Using links in this document

The PDF version of the guide provides links to other files or pages. Links are shown in blue text and operate as follows:

- Internal links within this document always work when you use the PDF version of this guide. Internal links include links to tables, figures, or other sections of the book.
- You can use the PDF version of the guide on a system that is connected to the Internet. If you do, you can click the link to any Web site address, such as http://www.avaya.com, to go directly to the site.

Trademarks

Avaya and the Avaya Logo are trademarks of Avaya Inc. and might be registered in certain jurisdictions. Unless otherwise specified, all trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc.

Microsoft is a registered trademark of Microsoft Corporation. All other trademarks are the properties of their respective owners.

Related resources

This section describes additional documentation and training available to you.

User documentation

For information about items in the documentation set for this product, go to the Avaya Support Web site at http://www.avaya.com/support. Always use the appropriate CD or book to obtain specific information about planning, installing, administering, or maintaining an Avaya system.

Technical assistance

The following technical assistance is available if needed.

Remote support center

Your project manager or systems consultant is responsible for providing you with the telephone number of the appropriate remote support center.

The following numbers are available for technical assistance with Avaya products and services:

- Within the United States and Canada: call 1-800-242-2121.

- Within any other country: call your local distributor.

Help on the system

Online help is available as follows:

- *MAS:* Use the Help menu, press **F1**, or click the **Help** button (if available) for the application or wizard you are in.
- *DCT:* Press the **Help** button on any page of the DCT application.

Training

For information about product training, go to the Avaya Web site at www.avaya.com and click **Support** > **Training and Certifications**.

How to comment on this book

Avaya is interested in your suggestions for improving this information. Use infodev@avaya.com to communicate with us.

Be sure to include the name, issue number, and date of this book:

Avaya Modular Messaging for Microsoft Exchange Release 5.2 Installation and Upgrades, Issue 1.4, February 2012.

Chapter 1: Preinstallation requirements

This chapter describes the prerequisites for installing Avaya Modular Messaging software in a Microsoft Exchange environment.

Topics in this chapter include:

- Software shipped with the system on page 2
- Obtaining the DCT data file on page 3
- Downloading required software and documentation on page 3
- Security considerations on page 6
- Test equipment recommendations on page 7
- Initial switch and LAN administration on page 8

For information on specifications, site requirements, switch and LAN demarcation points for an Avaya-provided server, see *Installing the Avaya S8800 Server for Modular Messaging*.

Software shipped with the system

The following software ships with each Modular Messaging system:

Table 1: Required Modular Messaging software that ships with the system

Disk	Purpose
Avaya Modular Messaging R5.2 MAS Application—2 DVDs	Use this software for: • Installing the Modular Messaging software, Text-to-Speech (TTS) software, and optional application programs running on Avaya-provided servers and customer-provided servers • Upgrading an MAS from Modular Messaging Release 3.x or Release 4.0 to Release 5.2 • Migrate an MAS from Modular Messaging Release 3.1, Release 4.0 or Release 5.1 to Release 5.2 • Recovering from a catastrophic disk failure
Avaya Modular Messaging Messaging Application Server (MAS) and Boot Software for Microsoft Exchange and IBM Domino (One DVD)	This software reinstalls the boot-image on an Avaya MAS in a Microsoft Exchange configuration. Make sure you have the correct version of the boot-image, S3500, S8730, or S8800 1U. For more information, see Appendix G: Reloading software on an Avaya MAS on page 321.

Obtaining the DCT data file

Usually a person responsible for installation planning uses the Modular Messaging Data Collection Tool (DCT) to create a DCT data file prior to the installation. This person might be the project manager, a customer representative, or other responsible party. The DCT data file has the extension **mmdct**, such as *sitefile.mmdct*. You will need the DCT data file to configure each MAS.

1. Obtain the DCT data file from the appropriate person.
2. Copy the DCT data file to a CD-ROM, DVD, or USB storage device such as a flash drive, memory stick, or equivalent that you carry to the customer site.

Note:

For more information about the DCT, see the DCT online help, or the printed document, *Avaya Modular Messaging Data Collection Tool Help*, available on the Avaya Support Web site.

Downloading required software and documentation

You must download and use the software and documentation described in this section to install or upgrade an Avaya Modular Messaging system. You can obtain most of this information only from the Avaya Support Web site. Download this information before you go to the customer site because some Modular Messaging sites do not have Internet access.

Important:

Always check the Avaya Support Web site at http://www.avaya.com/support for recent updates and current information before starting an installation or upgrade. Be aware that links and paths on the Avaya Support Web site might change.

The following topics explain how to download or print the required software and documentation from the web:

- Downloading software updates on page 4
- Downloading configuration notes on page 4
- Downloading the installation and upgrade checklists on page 5
- Downloading user documentation on page 5

You may require additional third-party software downloads for certain installation and upgrade procedures.

For information about downloading software required when installing Modular Messaging with Exchange 2007 or Exchange 2010 mail servers, see Completing MAS configuration prerequisites on page 46.

Downloading software updates

You must update the Avaya Modular Messaging software for each installation or upgrade to bring it up to date with the latest changes. To obtain the latest Avaya Service Pack (SP), software patches for the system:

1. Go to the Avaya Support Web site at http://www.avaya.com/support.
2. Download any files needed to update a Release 5.2 system. Ensure that you download any instructions required to install the Service Pack or software update.
3. In addition to any other files, download the following:
   - The latest DCT executable file (MMDCT.exe).
   - The latest Modular Messaging Release 5.2 Service Pack.
   - The latest Modular Messaging Release 5.2 patch.
   - Download the Modular Messaging Outlook Thick Client installation package.
4. Copy the downloaded files to a USB storage device such as a flash drive, memory stick, or equivalent.
5. Take the USB storage device with you to the installation site.

Downloading configuration notes

Obtain the configuration notes, which are required for integrating the MAS with the PBX or switch at this site. This information is available only on the Avaya Support Web site and must be obtained before you install the software. To obtain the most current copy:

1. Go to the Avaya Support Web site at http://www.avaya.com/support.
2. Download or print the configuration notes for the switch integration you need.

Note:

For AudioCodes gateway configuration notes, go to http://www.audiocodes.com/avaya Web site.

Downloading the installation and upgrade checklists

The Avaya Support Web site provides access to a PDF version of the installation and upgrade checklists. You can also find the checklists in Appendix A: Installation, upgrade, and migration checklists on page 225. To download the checklists:

1. Go to the Avaya Support Web site at http://www.avaya.com/support.
2. From the **File Download** dialog box, open or save the checklists file.

Downloading user documentation

You can obtain user documentation needed for installing or upgrading a system on the Avaya Support Web site:

1. Go to the Avaya Support Web site at http://www.avaya.com/support.
2. Click **Documentation** for a list of downloadable documents.
3. Either click to view or print files, or right-click to download the files you need:

Table 2: Modular Messaging documentation

Document
Avaya Modular Messaging Client Microsoft Outlook User Guide
Avaya Modular Messaging Concepts and Planning Guide
Modular Messaging MultiSite Guide
Avaya Modular Messaging Data Collection Tool Help
Avaya Modular Messaging Documentation library
Avaya Modular Messaging for Microsoft Exchange Release 5.2 Installation and Upgrades
Avaya Modular Messaging MAS Administration Guide
Avaya Modular Messaging Subscriber Options User Guide
Getting Started with Avaya PLDS
Installing the Avaya S8800 Server for Modular Messaging
Maintaining the Avaya S8800 1U Server for Modular Messaging
Maintaining the Avaya S8730 Server for Modular Messaging
Maintaining the Avaya S3500 Server for Modular Messaging

Table 2: Modular Messaging documentation (continued)

Document
Installing and configuring Avaya WebLM server
Avaya Modular Messaging Web Subscriber Options Server Installation
White paper for MM 5.1 with Windows 2008 support
Dialogic guides (to access use the Quick Install Cards Search Tool on the Intel Telecom Boards Web site)
Audiocodes gateway configuration notes. For the configuration notes, see http://www.audiocodes.com/avaya.

Security considerations

The following security-related issues apply to all Modular Messaging installations.

On-site security considerations

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

Password security

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 during installation

To protect system security during the installation:

- Remove all test subscribers and test mailboxes from the system when the procedures instruct you to do so.
- Always log off or lock the server if you leave it unattended, even for a short period of time.

- Give a copy of the most current DCT data file (*.*mmdct*) to the customer and the appropriate support organization after you finish an installation or upgrade. Afterwards, remove the DCT data file from your USB storage device or laptop.

Ongoing system security considerations

Customers are responsible for obtaining and installing antivirus software on any Microsoft Windows computer that is to run Avaya Modular Messaging software. Customers must also routinely install updates for the Microsoft Windows systems to protect the system from known security weaknesses. Updates include operating system updates and security patches. For more information, see "Modular Messaging and security"on the *Avaya Modular Messaging Documentation* library.

Note:

Avaya technical support representatives must follow their specified internal procedures for verifying the software that is installed. If required, they must update the software with the latest patches as instructed.

Test equipment recommendations

Recommended test equipment for a successful installation includes:

- At least two telephones connected through the switch or private branch exchange (PBX). The telephones must be of the same type as the majority of telephones the customer plans to use on the system.
  - Preferably the test telephones will have a data display for testing integration and the Find Me and Call Me features.
  - If the message waiting indicator (MWI) for the system is a lamp, the test telephones must be equipped with a lamp. If the MWI is a stutter tone, the telephones must be able to provide the stutter notification.
  - Place the test telephones so you can easily see the monitor while using the telephones.
- Access to a fax machine, if you plan to install MM Fax functionality.

Initial switch and LAN administration

This section describes the initial switch or Private Branch Exchange (PBX) and local area network (LAN) administration that is required. Customers must complete this administration before or during a new Avaya Modular Messaging installation.

CAUTION:

It is crucial to coordinate the IP addresses that are to be used with the Avaya Modular Messaging system with those on the corporate LAN. If you specify an IP address for a message server that conflicts with another Ethernet endpoint, the resulting traffic problems on the local area network can be extremely difficult to diagnose and solve.

Initial switch or PBX administration

Initial switch or PBX administration might or might not be complete when you arrive on site, depending on the contract or customer agreements. When you install a new server, the switch administration must support:

- Testing the system with at least one test subscriber.
- Cut to service procedures that provide the subscribers with an active coverage path.
- For configurations that use analog and DSE port boards, the ability for testers to call each channel individually. The appropriate party must test each channel to be connected to the system before assigning the channels to the server or another application.

Verify that initial switch administration and testing is complete before you start.

Initial LAN administration

The LAN administrator must administer the corporate LAN for the messaging system. Some LANs might be administered before the on-site installation starts. Other LANs require that the administration for a new server be done at the time of installation.

Note:

Avaya is not responsible for the installation, administration, or test of communications between customer computers and the LAN.

Chapter 2: Preparing to install Modular Messaging software

This chapter describes how to set up Modular Messaging accounts on the directory server and prepare the directory server to support the Modular Messaging software.The steps in this chapter must be completed by the directory server administrator or other authorized customer personnel before a technician can install Modular Messaging software on the first MAS in the system.

Topics in this chapter include:

- Overview on page 9
- Setting up Modular Messaging accounts on page 10
- Assigning permissions to the Modular Messaging service permissions group on page 17
- Creating MAS computer accounts on page 31
- Setting up each server for remote access on page 32
- Updating the Active Directory schema on page 33

Overview

This chapter describes the following system preparation steps:

1. For all installations, you must create a Modular Messaging security group, customer accounts and technical support accounts on the directory server and add the correct permissions for each account. For information about the correct permissions, see Appendix K: Administrator reference on page 351.
2. Depending on local requirements, you must create computer accounts for each MAS in the Active Directory and set up each MAS to allow remote access by technical support staff.
3. You must update the Active Directory schema before you install any Modular Messaging software on any Messaging Application Server (MAS) in the domain.

CAUTION:

All servers must meet the requirements listed in the *Avaya Modular Messaging Concepts and Planning Guide*. Review this document to verify that all Exchange servers, directory servers, MASs, and client machines are ready to support Modular Messaging software.

To successfully set up the Windows system to support the Modular Messaging software, you need:

- Access to the *Avaya Modular Messaging Messaging Application Server Software* media. To install a system with an Exchange 2010 peer mail server you must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
- The names and passwords for accounts and groups that will be created by the procedures in this chapter, including the customer account, Modular Messaging service permissions group, technical support account, and test subscribers. If necessary, see the Data Collection Tool data file for account and group names and passwords.

Setting up Modular Messaging accounts

You must create two Windows domain user accounts on the directory server to support Modular Messaging and you must assign sufficient permissions to the accounts.

- Create a customer account to install and administer the Modular Messaging software.
- Create a technical support account to allow remote support staff to access and administer the Modular Messaging system.

At this time you can also optionally create a test subscriber account for each Telephone User Interface (TUI) that will be used at this site. The test subscriber accounts are required to support acceptance testing after the MAS is configured.

Note:

If using Exchange 2007 mail server, you can use an Exchange PowerShell script to automate some of the steps to create and assign required permissions to the Modular Messaging accounts and service permissions group. For more information, see Using Power Shell to create a Modular Messaging service permissions group on page 16.

Creating Modular Messaging customer and technical support accounts

To prepare for creating customer and technical support accounts, complete the following steps:

1. Log on to the Active Directory server using an account that has privileges to create new user accounts (such as *administrator*).
2. Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** dialog box, expand the Windows domain you intend to use for Modular Messaging. This is the Corporate Windows domain entry in the DCT data file.

Creating the Modular Messaging customer account

To create the Modular Messaging customer account, you must first create a new security group (MM Service Permissions) and then create the customer account and assign appropriate permissions.

Creating the Modular Messaging service permissions group

Create a new security group (MM Service Permissions) that will give the Modular Messaging customer account the appropriate permissions. For example:

1. In the left pane, right-click **Active Directory Users and Computers**, **Users** > **New** > **Group**.
2. In the **New Object - Group** dialog box, create a new security group as follows:
   a. Enter the Modular Messaging service permissions group name (such as *MM Service Permissions*). For the correct value, see the Modular Messaging service permissions group field in the DCT file.
   b. Select the group scope appropriate for this site.
   c. Select group type **Security**. Click **Next**.
   d. On the next screen, do *not* create a mailbox (clear the check box if it is checked). Click **Next**.
   e. Click **Finish**.
3. In the left pane, click **Users**.
4. In the right pane, find the new group (such as *MM Service Permissions*) and double-click it.
5. In the **Properties** dialog box, click the **Member Of** tab.
   a. Click **Add**.
   b. In the **Select Groups** dialog box, add the following groups to assign the necessary permissions. Double-click each group to add it to the permissions list:
      - *Administrator* (required for the domain that contains the Global Catalog server that will be used as peer directory server for Modular Messaging)

        Note: This is the built-in administrators account. It is NOT the Windows domain administrator (Domain Admins) account.
      - *Account Operators* (required for each domain that will contain user accounts to be enabled for Modular Messaging)
      - *Exchange Recipient Administrators* (required only for the systems using Exchange 2007 mail servers)
      - Recipient Management and Public Folder Management (required only for the systems using Exchange 2010 mail servers)
   c. Click **OK** to close the **Select Groups** dialog box.

6. Click **OK** to close the **Properties** dialog box.

   To assign permissions to the service permissions group, see Assigning permissions to the Modular Messaging service permissions group on page 17.

Creating the Modular Messaging customer account

Create a new account for installing and administering the Modular Messaging software (this is the Modular Messaging customer account). For example:

1. In the left pane, right-click **Active Directory Users and Computers > Users** > **New** > **User**.
2. In the **New Object - User** dialog box, create a new Modular Messaging customer account using a secure logon name. For example:
   a. First name: Customer
   b. Last name: Account
   c. User logon name: *customer-provided* (such as *mmacct*). For the correct value, see the customer account field in the DCT file.

   Note:

   Ensure that you are satisfied with the Modular Messaging account names and passwords that you choose now. They are not easy to change later.

   d. Click **Next**.
   e. Enter and confirm the password.

   Note:

   Password policies vary from site to site. Consult your Windows administrator when selecting Modular Messaging account password. Do not create passwords composed of easily guessed words or numeric combinations, including sequential or repeated numbers. You must use a combination of at least three of the following character types: uppercase and lowercase letters, numbers, and special characters or symbols.

   f. Select **Password never expires**.

   Note:

   If you need to change the password for a Modular Messaging customer account at some point, contact the software-provider for the password-changing procedure.

   g. Click **Next**.
   h. On the following page, clear the check box for **Create an Exchange mailbox**.

   Note:

   You do not need to create an Exchange mailbox for a Modular Messaging customer account.

   i. Click **Next**.

j. When the summary is displayed, click **Finish**.

3. In the left pane, click **Users**.
4. In the right pane, locate the new account and double-click it.
5. In the **Properties** dialog box, click the **Member Of** tab.
6. Verify that the **Domain Users** entry is present. If the Domain Users entry is missing:
   a. Click **Add**.
   b. In the **Select Groups** dialog box, add **Domain Users** to this account.
   c. Click **OK** to close the **Select Groups** dialog box.

   Note:

   If you have used Powershell script for Exchange 2007, skip steps 7 and 8.
7. Add the customer account to the Modular Messaging service permissions group you just created:
   a. Click **Add**.
   b. In the **Select Groups** dialog box, add the Modular Messaging service permissions group that you just created (such as *MM Service Permissions*).
   c. Click **OK** to close the **Select Groups** dialog box.
8. Click **OK** to close the **Properties** dialog box.

Creating the Modular Messaging technical support account

Create a new account to allow remote support staff to access and administer the Modular Messaging system. For example:

1. In the left pane, right-click **Active Directory Users and Computers > Users** > **New** > **User**.
2. In the **New Object - User** dialog box, create a new Modular Messaging remote access account using a secure logon name. For example:
   a. First name: Support
   b. Last name: Account
   c. User logon name: *customer-provided* (such as *techacct*). If necessary, for the correct value, see the technical support account field in the DCT.
   d. Click **Next**.
   e. Enter and confirm the password.
   f. Select **Password never expires**.

   Note:

   If you ever change the password for the remote access account, be sure to notify the appropriate technical support organization.

g. Click **Next**.
h. On the following page, clear the check box for **Create an Exchange mailbox**.
i. Click **Next**.
j. When the summary is displayed, click **Finish**.

3. In the left pane, click **Users**.
4. In the right pane, double-click the name of the new account.
5. In the **Properties** dialog box, click the **Member Of** tab.
6. Verify that the **Domain Users** entry is present. If the Domain Users entry is missing:
   a. Click **Add**.
   b. In the **Select Groups** dialog box, add **Domain Users** to this account.
   c. Click **OK** to close the **Select Groups** dialog box.
7. Click **OK** to close the **Properties** dialog box.

Creating test subscriber accounts

Create at least one new test subscriber account for each telephone user interface (TUI) to be used at this site. The test subscriber accounts will be used for acceptance testing later in the installation. You may need to create up to three accounts, one for the MM Aria telephone user interface (TUI), one for the MM AUDIX TUI, and one for the MM Serenade TUI. For example:

1. In the left pane, right-click **Active Directory Users and Computers > Users > New** > **User**.
2. In the **New Object - User** dialog box, create a new account, such as:
   a. First name: *Aria Test*
   b. Last name: *Subscriber*
   c. User logon name: *customer-provided* (such as *testsub1*).
   d. Click **Next**.
   e. Enter and confirm the password for the account (*customer-provided*).
   f. Set up other parameters as required for this site.
   g. Click **Next**.
   h. On the third page, verify that **Create an Exchange mailbox** is selected.
   i. Select the required **Server** (Exchange organization) and **Mailbox Store** (Exchange server).
   j. Click **Next**.

k. When the summary is displayed, click **Finish**.

A new account is added to the list in the right pane.

Note:

The extension for the test subscriber must be administered on the PBX by the appropriate party.

3. Repeat Steps 1 and 2 to set up test subscribers for AUDIX and Serenade if required for this site.
4. Verify that the **Domain Users** entry is present. If the Domain Users entry is missing:
   a. Click **Add**.
   b. In the **Select Groups** dialog box, add **Domain Users** to this account.
   c. Click **OK** to close the **Select Groups** dialog box.
5. Click **OK** to close this dialog box.

Assign Modular Messaging characteristics to this account after the Modular Messaging software is installed. See Adding a test subscriber on page 108.

Using Power Shell to create a Modular Messaging service permissions group

For Exchange 2007 and Exchange 2010 environments or a mixture of both, you can use an Exchange PowerShell script to complete some tasks that are part of creating and assigning permissions to the Modular Messaging service permissions group. The PowerShell script can:

- Create the Modular Messaging service permissions group
- Assign the required Exchange Organization permissions to the group
- For Exchange 2007: Add the Modular Messaging service permissions group to the Exchange Recipient Administrators group.
- For Exchange 2010: Add the Modular Messaging service permissions group to the Recipient Management and Public Folder Management group.

Before you can use the script to create the security group, you must create the customer account and the technical support account. For more information, see Creating Modular Messaging customer and technical support accounts on page 10. Ignore the instructions for creating the Modular Messaging service permissions group, creating only the accounts. When creating the customer account ignore the steps for adding the account to the Modular Messaging service permissions group.

After creating the customer account and technical support account, complete the following steps to run the PowerShell script:

1. Download the correct script for your environment from the Avaya support site http://www.avaya.com/support. For Exchange 2007 installations, download the script named **createsecuritygroup.ps1**. For Exchange 2010 installations or a mixture of Exchange 2010 and Exchange 2007, download the script named **createsecuritygroupExch2010.ps1**.
2. Log on to the Exchange server using an account with Exchange Organization Administration privileges. In a mixed Exchange environments, log onto a Exchange 2010 server.

   Run the Exchange Management Shell. The script execution policy in Powershell may need to be updated to allow non-signed scripts to run. To set the execution policy, use the following command:
   set-executionpolicy remotesigned
   The system prompts you to confirm the changes.
3. Run the script with the following parameters in the listed order:
   - customer account name
   - technical support account name
   - Modular Messaging service permissions group name
   - Modular Messaging Service Permission Group alias

- container to create Modular Messaging service permissions group in
- domain name
- Exchange organization name

  For example: **C:\Avaya_Support\Exchange2010Migration> createsecuritygroup.ps1 'mmacct''mmtech''MM Service Permissions Group' 'MM Service Permissions Group' 'avaya.com/users''avaya.com''ExchangeOrg'**

  For information about using the Exchange Management Shell, see your Microsoft Exchange documentation.

After running the script, you must:

1. If running a mixed environment with Exchange 2007 and Exchange 2010, add the Modular Messaging service permissions group to the Exchange Recipient Administrators group.
2. Manually add the Modular Messaging service permissions group to the built in Administrators and Account Operators groups.
3. Manually assign *send as* permissions to the Modular Messaging service permissions group, see Assigning Send As permission on page 17.

Assigning permissions to the Modular Messaging service permissions group

Use the steps in this section to assign permissions to the Modular Messaging customer account by assigning permissions to the Modular Messaging service permissions group that you created in Creating the Modular Messaging service permissions group on page 11. Sufficient permissions must be assigned to the group for the customer account to function as required. For details on permission requirements, see Appendix K: Administrator reference on page 351.

To assign permissions to the Modular Messaging service permissions group, complete the following procedures:

- Assigning Send As permission on page 17
- Assigning additional permissions on page 19

Assigning Send As permission

You must assign *Send As* permission to the Modular Messaging service permissions group to allow Modular Messaging to deliver call answer messages to Modular Messaging enabled

mailboxes. For more information, see Send As permission on page 354. Complete the following steps to assign *Send As* permission:

1. Log on to the Active Directory server using an account that has Domain Administrator privileges.
2. Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
3. On the **View** pull-down menu, verify that **Advanced Features** is selected.
4. In the left pane of the **Active Directory Users and Computers** dialog box, select the domain and right-click. Select **Properties**.
5. On the **Properties** dialog box, select the **Security** tab.
6. Click **Advanced**.
7. On the **Advanced Security Settings** dialog box, click **Add**.
8. In the **Select Users, Computers, and Groups** dialog box, add the Modular Messaging service permissions group (such as *MM Service Permissions*).
9. Click **OK** to close this dialog box.
10. In the **Apply onto** field, select **User objects**.
11. In the **Permissions** box, allow **Send As** permissions
12. Click **OK** to close the **Permission Entry** dialog box.
13. Click **OK** to close the **Advanced Security Settings** dialog box.
14. Click **OK** to close the **Properties** dialog box.

A security descriptor is periodically applied to the protected groups and users listed below. As a result, *Send As* permissions are removed from these objects.

Protected Groups and Users:

- Administrators
- Account Operators
- Server Operators
- Print Operators
- Backup Operators
- Domain Admins
- Schema Admins
- Enterprise Admins
- Cert Publishers
- Administrator account
- Krbtgt account

If any of the protected groups and users listed above is enabled for Modular Messaging, complete the following steps to prevent *Send As* permissions from being removed. You must be a member of the domain administrators group to complete this procedure:

Note:

The dsacls utility is not standard with Windows Server 2003. It is part of the Windows 2003 support tools that ship on the Windows 2003 installation media.

1. Click **Start > Run**, enter **cmd** and click **OK**.
2. In the command window, enter the following:

   C:\Program Files\Support Tools>dsacls "cn=adminsdholder,cn=system,dc=*<xxx>*,dc=*<yyy>*" /G "*<MM Security Group>*:CA;Send As"

   where **dc=<xxx>,dc=<yyy>** is the customer's fully qualified domain name (for example, **dc=Avaya,dc=com**) and **<MM Security Group>** is the name of the Modular Messaging service permissions group.

   It will take at least an hour for the security permissions to replicate to the protected groups and their members.

Assigning additional permissions

Procedures for assigning permissions are different for Exchange 2003 and Exchange 2007 message stores. Select the procedure that applies to your environment:

- Assigning permissions with Exchange 2010 on page 19
- Assigning permissions with Exchange 2007 on page 22
- Assigning permissions with Exchange 2003 on page 24

Note:

If installing Modular Messaging into a mixed environment of Exchange 2007 and Exchange 2003, you must assign permissions for the version of Exchange running on the Exchange server being used as the Peer Messaging Server.

Assigning permissions with Exchange 2010

In a system with the Exchange 2010 mail server, you need to add the permissions that you want to assign to a group.

Note:

In systems with Exchange 2010 mail servers, the Modular Messaging service permissions group must be a member of the *Recipient Management and Public Folder Management* groups. For more information, see Creating the Modular Messaging service permissions group on page 11.

Adding permissions with Exchange 2010

Use **Active Directory Sites and Services** to add the required permissions. The permissions listed in step 14 are the absolute permissions required. You must match these permissions exactly. Adding permissions or removing some of the listed permissions could impact the installation and administration of the MM system. For convenience, create all the properties at the Exchange Organization level. You can apply these properties at a level lower down the tree.

To assign permissions to the Modular Messaging customer account:

1. Log on to the Active Directory server using an account, such as administrator, that has privileges to assign permissions to accounts.
2. Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Sites and Services**.
3. In the left pane, select **Active Directory Sites and Services**.
4. From the **View** menu, select **Show Services Node**. The menu item shows a check mark after you select it.
5. In the left pane:
   a. Expand **Services**.
   b. Expand **Microsoft Exchange**.
   c. Locate the Exchange Organization object that Modular Messaging will connect to.
   d. Right-click the Exchange Organization object and select **Properties**.
6. In the **Properties** dialog box, click the **Security** tab.

   Note:

   In an environment with both Exchange 2003 and Exchange 2010 mail servers, the **Security** tab may not be visible. Enable it by adding the **ShowSecurityPage** registry key. For more information see, Editing the registry on page 24. You can complete this procedure only on an MAS that has Exchange 2003 System Management Tools installed.

   Note:

   If the Security tab is not visible, you can use the ADSI edit to assign the permissions.
7. Click **Add**.
8. In the **Select Users, Computers, and Groups** dialog box, add the Modular Messaging service permissions group, such as *MM Service Permissions*.
9. Click **OK** to close this dialog box.
10. Under the **Permissions for the group** section, select the **Read** check box in the **Allow** column, and then click **Apply**.
11. Click **Advanced**.

12. In the **Advanced Security Settings** dialog box, on the **Permissions** tab, select the **Allow inheritable permissions from the parent to propagate to this object and all child objects** check box.
13. Click **Add**, and then add the Modular Messaging service permissions group (such as *MM Service Permissions*). Click **OK** to close the dialog box.
14. Complete the following steps to add permissions to the Modular Messaging service permissions group:
    a. In the **Apply onto** field, select **This object and children objects**.
    b. Verify that the **Apply these permissions to objects and/or containers within this container only** check box is not selected.
    c. In the **Permissions** box, allow the following permissions. Note that certain selections will result in the application of additional permissions. For details of these permission requirements, see Send As permission on page 354.
       - List contents
       - Read all properties
       - Write all properties
       - Read permissions
       - Create all child objects
       - Administer information store
       - Create named properties in the information store
       - Receive As
       - Send As
       - View information store status

       If you are running a mixed environment of Exchange 2003 and Exchange 2010 mail servers, also select the following permissions, which are only displayed for Exchange 2010 in the mixed environment:
       - Read
       - Execute
    d. Click **OK** to close the **Permission Entry** dialog box.
    e. Click **OK** to close the **Advanced Security Settings** dialog box.
    f. Click **OK** to close the **Properties** dialog box.

Assigning permissions with Exchange 2007

With an Exchange 2007 mail server, assign permissions to the group by adding the required permissions.

Note:

You may skip this section if you have already run the Exchange shell script. For more information Using Power Shell to create a Modular Messaging service permissions group on page 16

In systems with Exchange 2007 mail servers, the Modular Messaging service permissions group must be a member of the Exchange Recipient Administrators group. For more information, see Creating the Modular Messaging service permissions group on page 11.

Adding permissions with Exchange 2007

Use **Active Directory Sites and Services** to add the required permissions. The permissions listed in step 14 are the absolute permissions required. You should match these permissions exactly. Adding permissions or removing some of the listed permissions could impact the installation and administration of the MM system. For convenience, all the properties should be created at the Exchange Organization level. You can choose to apply the properties at a level lower down the tree if required.

To assign permissions to the Modular Messaging customer account:

1. Log on to the Active Directory server using an account that has privileges to assign permissions to accounts (such as *administrator*).
2. Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Sites and Services**.
3. In the left pane, select **Active Directory Sites and Services**.
4. From the **View** pull-down menu, select **Show Services Node** (the menu item shows a check mark after you select it).
5. In the left pane, expand **Services**, expand **Microsoft Exchange**, and then locate the appropriate *Exchange Organization* object that Modular Messaging will connect to. Right-click it and select **Properties**.
6. In the **Properties** dialog box, click the **Security** tab.

   Note:

   In an environment with both Exchange 2003 and Exchange 2007 mail servers, the Security tab may not be visible. Enable it by adding the **ShowSecurityPage** registry key. For more information see, Editing the registry on page 24. You can complete this procedure only on an MAS that has Exchange 2003 System Management Tools installed.

Note:

ADSI edit can also be used to assign these permissions if the **Security** tab is not visible.

7. Click **Add**.
8. In the **Select Users, Computers, and Groups** dialog box, add the Modular Messaging service permissions group (such as *MM Service Permissions*).
9. Click **OK** to close this dialog box.
10. Under the **Permissions for the group** section, select the **Read** check box in the **Allow** column, and then click **Apply**.
11. Click **Advanced**.
12. On the **Advanced Security Settings** dialog box, on the **Permissions** tab, check the box at the bottom of the dialog box that will **Allow inheritable permissions from the parent to propagate to this object and all child objects**.
13. Click **Add** and add the Modular Messaging service permissions group (such as *MM Service Permissions*). Click **OK** to close the dialog box.
14. Complete the following steps to add permissions to the Modular Messaging service permissions group:
    a. In the **Apply onto** field, select **This object and children objects**.
    b. Verify that the following box is *not* checked, **Apply these permissions to objects and/or containers within this container only**.
    c. In the **Permissions** box, allow the following permissions. Note that certain selections will result in the application of additional permissions. For details on these permission requirements, see Send As permission on page 354
       - List contents
       - Read all properties
       - Write all properties
       - Read permissions
       - Create all child objects
       - Administer information store
       - Create named properties in the information store
       - Receive As
       - Send As
       - View information store status

       If you are running a mixed environment of Exchange 2003 and Exchange 2007 mail servers, also select the following permissions, which are only displayed for Exchange 2007 in the mixed environment:

- Read
- Execute

d. Click **OK** to close the **Permission Entry** dialog box.

e. Click **OK** to close the **Advanced Security Settings** dialog box.

f. Click **OK** to close the **Properties** dialog box.

Assigning permissions with Exchange 2003

With an Exchange 2003 mail server, to assign permissions to the group, you must:

1. Edit the registry to display the **Security** tab.
2. Add required permissions.

Editing the registry

By default, the **Security** tab for the Exchange organization container and some of the key sub containers are not visible using Exchange System Manager or Active Directory Sites and Services. The following registry change enables the **Security** tab at all levels within the Microsoft Exchange container.

To update the registry:

1. Log on as the Microsoft Exchange administrator.
2. Click **Start** > **Run**.
3. In the **Run** dialog box **Open** field, type **regedit** and press **Enter**.
4. In the **Registry Editor** dialog box, locate the following key:

   HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin
5. Right-click **ExAdmin** and select **New** > **DWORD Value**.
6. Enter the following value name: **ShowSecurityPage**
7. Double-click the **ShowSecurityPage** value.
8. In the **Edit DWORD Value** dialog box, set the Value data to **1**.
9. Click **OK** to close this dialog box.
10. Click **OK** to close the **Registry Editor** dialog box.

Adding permissions with Exchange 2003

Use **Active Directory Sites and Services** to add the required permissions. The permissions listed in Step 7 are the absolute permissions required for the Modular Messaging software to function. For convenience, all the properties should be created at the Exchange Organization level. You can choose to apply them at a level lower down the tree if required, but this might affect your ability to manage Modular Messaging using Exchange System Manager.

To assign permissions to the Modular Messaging customer account:

1. Log on to the Active Directory server using an account that has privileges to assign permissions to accounts (such as *administrator*).
2. Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Sites and Services**.
3. In the left pane, select **Active Directory Sites and Services**.
4. From the **View** pull-down menu, select **Show Services Node** (the menu item shows a check mark after you select it).
5. In the left pane, expand **Services**, expand **Microsoft Exchange**, and then locate the appropriate *Exchange Organization* object that Modular Messaging will connect to. Right-click it and select **Properties**.
6. In the **Properties** dialog box, click the **Security** tab. This tab is visible only if you edited the registry as directed in the previous procedure.
   a. Click **Add**.
   b. In the **Select Users, Computers, and Groups** dialog box, add the Modular Messaging service permissions group (such as *MM Service Permissions*).
   c. Click **OK** to close this dialog box.
7. Under **Permissions** for the group, **Allow** the permissions listed below. For details on these permission requirements, see Appendix K: Administrator reference on page 351.

   Note:

   You may find it easier to verify the permissions by working from the bottom of the list to the top.

   - Read
   - Execute
   - Read permissions
   - Create children
   - List contents
   - Read properties
   - Write properties
   - Administer information store
   - Create named properties in the information store
   - View information store status
   - Receive As
   - Send As
8. Click **Apply** to verify the settings.
9. Click **OK** to close this dialog box.

10. Close the **Active Directory Sites and Services** dialog box.
11. Wait for the directory cache to expire.

Preparing Exchange 2010

To configure an Exchange 2010 server to function as a Modular Messaging peer or as a non-peer Exchange server, you need to perform the following tasks:

Note:

The customer account name used in this section is mmacct. In the commands and examples below, substitute this name with the correct customer account for the Modular Messaging implementation. If there is more than one account listed in the Service Account group created for Modular Messaging, you should rerun each command for each of the accounts.

Note:

To complete many of the steps below, you require a higher permissions level than what is typically available to an implementation engineer. Most steps will also require access to the Exchange Management Shell for Exchange 2010, which is not available on the MAS. You can complete this section at any time prior to integrating Modular Messaging with Exchange 2010.

- **Set permissions for service account:**

  The service account group requires additional security groups added to it. You must add the following security groups:

  - Recipient Management
  - Public Folder Management

- **Enable remote scripting:**

  Exchange 2010 supports remote administration using Remote PowerShell, but only PowerShell 2.0 supports this feature. By default, remote scripting is disabled for all users. You must enable remote scripting for the service account in order for it to automatically create Modular Messaging specific system accounts and associated mailboxes. This is because the Exchange Management Powershell Snap-in cannot be used on the MAS.

  To enable remote scripting for the service account, run the following command on the Exchange management shell for Exchange 2010.

  ```
  Set-User mmacct -RemotePowerShellEnabled $True
  ```

- **Create Exchange Public Folders:**

  During the installation of Exchange 2010, customers can choose whether or not Public Folders should be available. However, when using MAPI/CDO, public folders are required on the server running Exchange 2010.

  If the public folders are not configured, then perform the following steps to create a public folders database:

  - Open the Exchange Management Console for Exchange 2010.

- Navigate to **Microsoft Exchange** > **Microsoft Exchange On-Premises** > **Organization Configuration** > **Mailbox** from the left pane of the Exchange Management Console.
- In the right pane of the Exchange Management Console, click **Database management**.
- From the list of actions, click **New Public Folder Database**.
- Follow the prompts to create the public folder database and then mount it.

- **Configure the Throttling policy:**

  Exchange 2010 uses client throttling policies to track the bandwidth that each Microsoft Exchange user consumes and to enforce bandwidth limits. Exchange administrators can use throttling policies to control the resources that can be used by a user. Since Modular Messaging runs under a service account and performs different interactions with Exchange on behalf of end users, the service account must bypass the throttling policies imposed by Exchange 2010. Service Pack 1 for Exchange 2010 includes additional methods for accomplishing that are not available in the GA version.

  To configure the throttling policy for the service account, run the following sequence of commands on the Exchange management shell for Exchange 2010.

  a. Create a new Throttling policy using the following command.

  ```
  "New-ThrottlingPolicy -name"Avaya_MM_ThrottlingPolicy"
    -RCAPercentTimeInAD $null -RCAPercentTimeInCAS $null
    -RCAPercentTimeInMailboxRPC $null –RCAMaxConcurrency $null"
  ```

  b. Attach the newly created throttling policy to the service account.

  ```
  Set-ThrottlingPolicyAssociation -Identity mmacct
    -ThrottlingPolicy "Avaya_MM_ThrottlingPolicy"
  ```

- **Create Management role:**

  Microsoft Exchange 2010 introduces a Role Based Access Control permissions model. Since the service account requires permission to act on behalf of end users, a new Management Role is required. Use the following command on the Exchange management shell for Exchange 2010 to create the required role:

  ```
  New-ManagementRoleAssignment -Name "Avaya_MM_ImpersonationRole"
    -Role ApplicationImpersonation -User mmacct
  ```

- **Configuring CAS servers to allow remote PowerShell using “Negotiate” Authentication mode:**
  Exchange Management Tools for Exchange 2010 are not available in the 32bit version, so you should perform the operations that require Exchange Management Tools using Remote PowerShell from the MAS server.

  Remote PowerShell uses Kerberos as a default authentication mechanism. To enable remote PowerShell to use “Negotiate” authentication mechanism, perform the following steps on each of the CAS servers.

1. Open **IIS Services Manager**.
2. Navigate to the **Default Web Site**.
3. Navigate to the **Powershell virtual** directory.
4. Double-click **SLL Settings** to open the **SSL settings** page.
5. Clear the **Require SSL** check box for Powershell virtual directory and click **Apply** in the **Actions** pane to apply the new settings.
6. Close **IIS Services Manager**.
7. Click **Start**, and then click **All Programs**.
8. Click **Accessories**, and then click **Command Prompt**.
9. At the Command Prompt, type ***cd %windir%\system32\inetsrv***, and then press **Enter**.
10. At the Command Prompt run the following commands.

```
appcmd set config "Default Web Site/PowerShell"
  -section:system.webServer/security/authentication/
  windowsAuthentication /enabled:"True" /commit:apphost

appcmd set config "Default Web Site/PowerShell"
  -section:system.webServer/security/authentication/
  windowsAuthentication /+"providers.[value='Negotiate']" /
  commit:apphost

appcmd set config "Default Web Site/PowerShell"
  -section:system.webServer/security/authentication/
  windowsAuthentication /+"providers.[value='NTLM']" /
  commit:apphost

appcmd set config "Default Web Site/PowerShell"
  -section:system.webServer/security/authentication/
  windowsAuthentication /
  +"providers.[value='Negotiate:Kerberos']" /commit:apphost
```

Note:

In some cases, these commands may result in an error message, such as "Cannot add duplicate collection entry of type 'add' with unique key attribute," and so on. This error is caused because the attribute has already been set and does not need to be updated. Using the 'List' command can display the current settings. For example,

```
appcmd list Config "Default Web Site/Powershell"
  -section:system.webServer/security/authentication/
  windowsAuthentication."
```

- **Ensure that the NTLM compatibility level is set correctly:**

  Modular Messaging requires that the NTLM compatibility level is set to allow clients to only use NTLM v2 authentication. On each MAS, manually set the following registry value to a data value of 3. The default is 2.

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\ lmcompatibilitylevel

Creating MAS computer accounts

Before the Modular Messaging software is installed, the domain administrator must create computer accounts for each MAS and supplementary server that are to be installed and define the Modular Messaging customer account as a user that has permission to join the Windows domain. This procedure facilitates remote access setup (see Setting up each server for remote access on page 32) and Modular Messaging software installation.

For example, to add a new computer account to the Active Directory on a Windows 2003 or 2008 system:

1. Log on to the Active Directory server using an account that has privileges to add a computer account to a domain (such as *Administrator*).
2. Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** dialog box, expand the directory for the Windows domain that you will use for Modular Messaging.
4. To create a new computer account, right-click **Computers**, and then select **New** > **Computer**.
   a. In the **New Object - Computer** dialog box, type the computer name for the MAS.
   b. Click **Next**.
   c. Do not select “this is a managed computer.” Click **Next**.
   d. Click **Finish** to close this dialog box.
   e. In the left pane, click **Computers**.
   f. Right-click the computer name. Select **Properties**. In the **Properties** dialog box, select the **Managed by** tab.
   g. Click **Change** to specify that a different user or group can add this computer to the domain.
   h. In the **Select User or Group** dialog box, enter the customer account name (such as *mmacct*). Then click to select that name.
   i. Click **OK** to close this dialog box.
   j. Click **OK** to close the **Properties** dialog box.
5. If more than one MAS is to be installed, repeat Step 4 until all MASs are added.

Setting up each server for remote access

Remote access allows technical support staff to dial into a system to correct problems and perform routine maintenance. Unless other arrangements were made, use the following procedure to allow each Modular Messaging server to support remote access calls.

1. The **Active Directory Users and Computers** dialog box should already be open. If not, repeat Steps 1 through 3 in Creating MAS computer accounts on page 31 to log on to an account with the appropriate privileges and access the Active Directory.
2. In the left pane of the **Active Directory Users and Computers** dialog box:
   a. Expand the directory for the domain that will be used for Modular Messaging.
   b. Click **Users**.
3. In the right pane, double-click **RAS and IAS Servers**.
4. In the **RAS and IAS Servers Properties** dialog box:
   a. Click the **Members** tab.
   b. Click **Add**.
   c. In the **Select Users, Contacts, Computers, or Groups** dialog box, double-click the entry for this server (for example, *MYMAS1*). It has a blue terminal icon.
   d. Verify that the correct computer name is shown underlined in the list box.
   e. Repeat Steps c and d to add all Modular Messaging servers to this list.
   f. Click **OK** to close this dialog box.
   g. Click **OK** to close the **RAS and IAS Servers Properties** dialog box.
5. In the right pane, double-click the account to be used for remote technical support, such as example *Services Account* or *Support Account*.
6. In the **Properties** dialog box for the remote access account:
   a. Click the **Dial-in** tab.
   b. Under **Remote Access Permission (Dial-in or VPN)**, select **Allow access**.
   c. Leave CallBack Options set at **No Callback**.
   d. Close this and the next dialog box.

Updating the Active Directory schema

Complete this task only once in the Active Directory *Forest*, on a domain controller, before installing the Modular Messaging software on any MAS.

The Active Directory must be updated as described in this section.

Note:

This procedure can be done only on a machine that is running the Windows 2000, 2003, or 2008 Server operating system. These components cannot be installed on a workstation OS.

To complete this update, you must log on to a domain controller using an account that has permission to complete Active Directory schema administration. This is usually the Windows domain administrator account. The account must have both Domain Admin and Schema Admin rights. The schema defines the objects and properties stored in Active Directory, and contains definitions of object attributes.

For details about the changes made to the schema for a Modular Messaging software update, see Appendix K: Administrator reference on page 351.

CAUTION:

If you do not update the schema first when required, the Modular Messaging software does not install correctly. It needs to be completely removed and then reinstalled following an Active Directory schema update.

Logging on and preparing to update

To update the Active Directory for Modular Messaging:

1. Log on to a domain controller.
   - If you are updating the Active Directory schema in a child domain, the account must have Domain Admin rights for both the parent domain and the child domain. If the Active Directory update is executed from the child domain controller, enter the account name in the format: *Parent Domain\Domain Admin*.
   - If you are using Octel Analog Networking with an Exchange 2003 message store, this procedure must be performed on the domain controller that is acting as the schema master. Octel Analog Networking is not supported with Exchange 2007 and Exchange 2010. However, Octel Analog Networking can be used in mixed Exchange environments as long as the VMD host is Exchange 2003.
2. Close applications or stop monitoring as follows:
   - Close the Active Directory Users and Computers application and the Microsoft Exchange System Management Tools.

- Close any open dialog boxes for other applications.
- Stop any monitoring tools that are running, such as antivirus software.

Adding the Schema Update registry key

This procedure is required when applying schema updates on a domain controller. Complete the following steps to add the registry key that will allow schema updates:

1. Click **Start** > **Run**.
2. In the **Run** dialog box **Open** field, type **regedit** and press **Enter**.
3. In the **Registry Editor** dialog box, locate the following path:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters
4. In the right panel look for the REG_DWORD Name **Schema Update Allowed**. If it exists, double-click it and verify that the **Value data** field is set to **1**.
5. If the DWORD value does not appear in the right panel, right-click **Parameters** and select **New** > **DWORD Value**.
6. Enter the following name: **Schema Update Allowed**.
7. Double-click the **Schema Update Allowed** value.
8. In the **Edit DWORD Value** dialog box, set the **Value data** to **1**.
9. Click **OK** to close this dialog box.
10. Click **OK** to close the **Registry Editor** dialog box.

Running the Modular Messaging installation wizard

When all preparations are complete, run the Modular Messaging Installation wizard as follows:

1. Insert the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1) into the DVD drive of the domain controller. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
2. Run the Modular Messaging Installation wizard as follows:
   a. Navigate to the **Install** directory on the DVD drive.
   b. Double-click the file **Setup.exe**.
3. On the main screen, verify that the Configuration drop-down box shows **Microsoft Exchange**.

Updating the Active Directory

To update the Active Directory schema on this machine:

1. Click the plus sign (**+**) to expand the **Active Directory updates** folder.

   Note:

   Do this task only once in the Active Directory Forest.

2. Select the following check boxes to install the appropriate software components to support Modular Messaging:

   - *Enable Modular Messaging:* Click this box to enable extension data replication among Active Directory servers. This allows Modular Messaging to store subscriber configuration information and support the correct operation of and access to client applications.
   - *Enable Octel Analog Networking:* For the systems using an Exchange 2003 message store, if Octel Analog Networking is used at this site, click this box to add the appropriate classes and attributes to the schema. This causes a Modular Messaging Octel Analog Networking tab to appear in the Microsoft Exchange administration program. Octel Analog Networking is not supported for Exchange 2007 and Exchange 2010. However, Octel Analog Networking can be used in mixed Exchange environments as long as the VMD host is Exchange 2003.
   - *Enable User Administration:* Click this box to enable objects that will appear on the Modular Messaging tab in the Active Directory. This allows administrators to use Microsoft Exchange administration to enable Modular Messaging features for users, groups, or contacts.

   Note:

   Although Octel Analog Networking is an optional feature, you might choose to install it at this time in case Octel Analog Networking is ever added to the system. The other schema updates are always required.

3. When all required components are selected, click **Install**.
4. Each component you select causes a Modular Messaging Active Directory installation wizard to run. Complete each wizard as follows:

   a. On the welcome screen, click **Next**.

   b. If prompted, enter the name and password of an account that has both Domain Admin and Schema Admin rights. (For example, *windowsdomain**schemaAdmin* and password.) Click **Next**.

   c. After the Active Directory registration process is complete, click **Next**.

   d. To complete the wizard, click **Finish**.

   e. Repeat Steps a through d for each occurrence of the wizard.

5. When component installation is complete, click **Close**.

6. Continue with Chapter 3: Adding Exchange extensions for Modular Messaging on page 37.

Configure NSPI for Windows Server 2008 domain controllers:

With Microsoft Windows Server 2008, the number of NSPI connections from an individual user is limited to 50. An NSPI connection is required for each MAPI logon, and if a user limit, is reached then that log-on attempt fails. In Modular Messaging, the service account performs all the logons for all the mailboxes, so this limit is too small. You must increase this limit on every Windows Server 2008 Domain Controller that Exchange may interact with. For more information on this topic, see the Modular Messaging Concepts and Planning Guide for Release 5.2.

For more details regarding NSPI connections and how to set the connection limit see the Microsoft Knowledge Base article, http://support.microsoft.com/kb/949469.

Note:

Introduction of Exchange 2010 does not increase the NSPI demands, so if the NSPI limit was set when Windows 2008 was introduced, no further changes are required.

Chapter 3: Adding Exchange extensions for Modular Messaging

This chapter describes how to install the Microsoft Exchange extensions that support user administration for Modular Messaging software. Installing the Subscriber Administration extensions creates a Modular Messaging tab in the Active Directory. However, the page is not functional until the Modular Messaging software is installed and operational.

Do this task on any machine that you will use for administering subscribers (such as the Exchange server, an MAS, or a client machine). You can do this task multiple times per network.

Note:

To add the extensions to an MAS after you install the Modular Messaging software, see Adding the Exchange extensions after installing the Modular Messaging software on page 43.

CAUTION:

Installing Modular Messaging for Exchange Administration extensions on a DC may require a server restart.

Topics in this chapter include:

- Overview on page 38
- Adding the Exchange extensions on page 40

Overview

This task assumes that you have already created a Modular Messaging customer account and updated the directory server as described in Chapter 2: Preparing to install Modular Messaging software on page 9.

CAUTION:

If the Active Directory has not been updated as described in Chapter 2: Preparing to install Modular Messaging software on page 9, do not proceed with the steps in this chapter. The Modular Messaging software will not install correctly, and it will have to be completely removed and reinstalled after the Active Directory updates have been made.

To successfully install the Modular Messaging Microsoft Exchange Subscriber Administration extensions, you need:

- Access to the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1). To install a system with an Exchange 2010 peer mail server you must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
- Downtime scheduled for the Microsoft Exchange 2003 server: This release of Exchange does not require the Subscriber Administration extensions or Octel Analog Networking Administration component to be installed on the Exchange server. If you choose to install them, the Exchange server may need to be restarted (see the following note).

Note:

You can install the Modular Messaging Subscriber Administration extensions component on any machine that has the Microsoft Exchange 2003 System Management Tools installed.

To use the Modular Messaging Active Directory Extensions for administration, you must have sufficient rights on the Active Directory to modify users.

Note:

If Octel Analog Networking is used at this site, you can install the Octel Analog Networking Administration component on any machine where the Microsoft Exchange System Management Tools are installed.

You cannot install the Modular Messaging Microsoft Exchange Subscriber Administration extensions on the Exchange 2007 server or Exchange 2010 server.

- **Exchange 2007 server***:* Modular Messaging Subscriber Administration Extensions are not supported on 64 bit Windows Server 2003 and on 64 bit Windows Server 2008.

  Install the Modular Messaging Subscriber Administration extensions component on a machine that has the Microsoft Exchange 2007 Management Tools installed. Modular Messaging supports installation of the tools only on machines running a 32-bit operating system. You must install the 32-bit version of the Exchange 2007 Management Tools,

which can be downloaded from Microsoft. For more information about downloading and installing the Exchange 2007 Management Tools, see Installing third-party software on page 51.

The Subscriber Administration extensions add a Modular Messaging tab to the Active Directory Users and Computers property page that is used for Modular Messaging subscriber administration. For a system running on Windows Server 2008 based Active Directory, the tab does not get added. If you have a system running on Windows 2008 based Active Directory, you can install Subscriber Administration Extensions on any other machine in the same domain, including a Windows 2008 member server, and use it to set up and administer Modular Messaging accounts.

Any machine on which you install the Subscriber Administration extensions may require a restart.

To use the Modular Messaging Active Directory Extensions for administration, you must have sufficient rights on the Active Directory to modify users.

CAUTION:

All servers must meet the requirements listed in the *Avaya Modular Messaging Concepts and Planning Guide*. Review this document to verify that all Exchange servers, directory servers, MASs, and client machines are ready to support Modular Messaging software.

- **Exchange 2010 server***:* 64-bit Windows Server 2003 and 64-bit Windows Server 2008 do not support Modular Messaging Subscriber Administration Extensions.

  The Subscriber Administration extensions add a **Modular Messaging** tab to the **Active Directory Users and Computers** property page. Use this tab for Modular Messaging subscriber administration. For a system running on Active Directory based on Windows Server 2008, the tab does not get added. If your system runs on Active Directory based on Windows 2008, you can install Subscriber Administration Extensions on any other computer in the same domain, including a Windows 2008 member server, and use it to set up and administer Modular Messaging accounts.

  Once the MAS installation is complete, you can install the Subscriber Administration extensions on any MAS other than the MAS on which Microsoft Exchange 2010 is installed. The MAS on which you install the Subscriber Administration extensions may require a reboot.

  To use the Modular Messaging Active Directory Extensions for administration, you must have sufficient rights on the Active Directory to modify users.

CAUTION:

All servers must meet the requirements listed in the *Avaya Modular Messaging Concepts and Planning Guide*. Review this document to verify that all Exchange servers, directory servers, MASs, and client machines are ready to support Modular Messaging software.

Adding the Exchange extensions

Complete this task for any machine that you will use for administering subscribers (such as the Exchange server, or a client machine). You can do this task multiple times per network.

Update the Microsoft Exchange extensions as follows:

- *For new installations:* Install these tools on the Exchange server, or other machine where they are required.
- *For upgrades:* Update the Exchange extensions software on any machines where it is installed.

Note:

Review the conditions for installing these Modular Messaging software components in the Overview on page 38. For an MAS, you will install the Subscriber Administration extensions component when you install the rest of the Modular Messaging software. See Chapter 4: Configuring an Avaya MAS on page 45, or Chapter 5: Configuring a customer-provided MAS on page 59.

*Although this procedure creates a Modular Messaging tab in the Active Directory, the page will **not** be functional until after the rest of the Modular Messaging software is installed and operational.*

Logging on and preparing to update

To update the Microsoft Exchange extensions for Modular Messaging:

1. Log on to the appropriate machine using an account that has permission to install software.
2. Close applications and stop monitoring on this machine as follows:
   - Close the **Active Directory Users and Computers** window, if that application is installed on this machine.
   - Close any open Exchange applications including the Microsoft Exchange Management Tools.
   - Close any open windows for other applications.

- Stop any monitoring tools that are running, such as antivirus software.

Running the Modular Messaging installation wizard

When all preparations are complete, run the Modular Messaging Installation wizard:

1. Insert the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1 of 2) into the DVD drive of this machine. When installing a system with an Exchange 2010 peer mail server you must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
2. To run the Modular Messaging Installation wizard:
   a. Navigate to the DVD drive (such as D:) and, from there, to the **Install** directory.
   b. Double-click the file **Setup.exe**.
3. On the main screen, verify that the Configuration drop-down box shows **Microsoft Exchange**.

Adding the Exchange extensions

To add the Exchange extensions tools to this machine:

1. Click the plus sign (**+**) to expand the appropriate Exchange extensions folder. Select the Exchange extensions:
   - Active Directory/Exchange 2007 extensions (Exchange 2003)
2. To install the Modular Messaging software components required for Microsoft Exchange systems on this machine, select the appropriate check box:
   - *Octel Analog Networking Administration:* If Octel Analog Networking is used at this site, click this box to allow administrators to administer an Octel Analog Networking gateway. This allows Modular Messaging subscribers to exchange voice messages with any other Octel Analog Networking-enabled voice mail system. Not supported with Exchange 2007 and Exchange 2010.
   - *Subscriber Administration:* Click this box to add a Modular Messaging property page in Active Directory Users and Computers for each user that is assigned a mailbox. This tool allows administrators to set up and administer Modular Messaging accounts, configure subscriber properties, and run the MM Client software (the Subscriber Options package).
3. When all required components are selected, click **Install**.
4. When all components finish installing, click **Close**.
5. If you are prompted to restart the system, click **Restart**.

Note:

After the Modular Messaging for Exchange Subscriber Administrator extensions are installed, a Modular Messaging tab appears. However, it is not functional until installation of the MAS is complete.

Adding the Exchange extensions after installing the Modular Messaging software

If you have already installed Modular Messaging Service Pack, you must perform the following steps to add the Exchange subscriber extensions, without the need to downgrade the Modular Messaging system to the release 5.0.

To add the Exchange extensions after installing the Modular Messaging software:

1. Insert the **MAS Apps Media DVD** into the DVD drive.
2. From the command prompt, execute the msi for Subscriber Admin tools using the following command:

   Note:

   The msi is located in the MAS Apps under the DVD drive:*Install**Exch2000 User Admin.*You can copy and paste these commands from this guide to the MAS to avoid any mistakes in the syntax of these commands. The following command is on one line.

   ```
   msiexec /i gv_subadmin.msi UM_CONTROLPANELNAME="MM Subscriber
     Administration" UM_COMPONENTNAME="Subscriber Administration
     Extensions" /qn
   ```

   The installation takes place in the background. This step can take 5 to 10 minutes to complete. Using Task Manager, wait until none of the msiexec processes remain running, and then perform the next step.
3. Upgrade the Subscriber Admin to the latest version by running the following command at the command prompt.

   ```
   MM52XX00.exe -guid={9683B7CD-9843-42b0-97A5-22C2421F98CB}
   ```

   Where XX is the service pack number.

   For installing the Subscriber Administration Extensions using Service Pack 8, the command is:

   ```
   MM520800.exe -guid={9683B7CD-9843-42b0-97A5-22C2421F98CB}
   ```

   The Exchange subscriber extensions are installed.

Chapter 4: Configuring an Avaya MAS

This chapter applies only to an Avaya-provided Messaging Application Server (Avaya MAS) and supplementary server installation. This chapter describes Modular Messaging MAS installation on an Avaya provided hardware.

If you are installing a customer-provided MAS, do not use the procedures in this chapter, see Chapter 5: Configuring a customer-provided MAS on page 59.

Topics in this chapter include:

- Completing MAS configuration prerequisites on page 46
- Displaying an MAS from the console on page 48
- Configuring MASs using an existing DCT data file on page 49
- Completing the MAS configuration on page 54
- Continuing the installation on page 57

Completing MAS configuration prerequisites

You must configure each new Avaya Messaging Application Server (Avaya MAS) for local operating settings and to work correctly on the corporate local area network (LAN) as described in this section. In addition, you must prepare it to operate correctly in the Microsoft Windows and Exchange environment.

The majority of the MAS configuration is automated by the Modular Messaging Configuration Wizard (MMCW). The MMCW configures the MAS from information in a site-specific configuration file, called a Data Collection Tool (DCT) data file (**.mmdct*). This file is created using the DCT executable file (MMDCT.exe). Typically the DCT data file is created prior to the installation by the project manager, customer administrator, and other experts responsible for the installation.

See the DCT online help system or its printed version, *Avaya Modular Messaging Data Collection Tool Help*, for a complete description of the procedure and specifications for creating a DCT data file.

Note:

Always check the Avaya Support Web site at http://www.avaya.com/support for recent updates to the DCT executable file (MMDCT.exe).

To successfully set up an Avaya MAS, you need:

- A complete and valid DCT data file.
- All the required system hardware are installed; see *Installing the Avaya S8800 Server for Modular Messaging* guide.
- A printout of the Avaya MAS installation checklist (see New Modular Messaging installation on an Avaya MAS on page 226). Check off steps as you complete them to track your progress.
- Avaya Modular Messaging 5.2, MAS for Microsoft® Exchange® & IBM Domino®, Boot Disk for recovery of existing image only.
- The following software from the Avaya Support Web site at http://www.avaya.com/support. For more information about how to access these items on the Web site, see Downloading required software and documentation on page 3.
  - Avaya software updates that are required to bring the Modular Messaging software up to date after an installation. Download this software to a USB storage device. For more information about downloading the updates, see Downloading required software and documentation on page 3.
  - The latest copy of the DCT executable file (**MMDCT.exe**). Download the file from the Avaya support Web site to a USB storage device. Download the executable file to the same USB storage device as the DCT data file.
  - The Modular Messaging 5.2 Client software.

- WebLM server installed, if you choose to install the WebLM on a standalone server. For instructions, see *Installing and configuring Avaya WebLM server*.
- New Modular Messaging license file obtained and applied on the WebLM server, if you are installing WebLM on a standalone server or using an existing WebLM server. For more information, see:
  - Obtaining the license file on page 91
  - Applying license file on the WebLM server on page 91
- To install a MAS with Exchange 2010 mail servers, you need:
  - MAPI Client v6.5.8190 or later
  - Microsoft Management Console 3.0
  - .NET 3.5 SP1
  - PowerShell 2.0
- For installing a system with Exchange 2007 mail servers, you need:
  - The 32-bit version of the Exchange 2007 Management Tools, Microsoft Exchange 2007 Service Pack 1, and additional software downloads. You may download the 32-bit version of the Exchange 2007 Management Tools from:

    http://www.microsoft.com/downloadsdetails.aspx?FamilyID=444C259E-605F-4A82-96D5-A2F448C9D4FF&displaylang=en
  - Microsoft Exchange Server MAPI Client for Microsoft Exchange 2007. Download the MAPI from the following site:

    http://www.microsoft.com/downloads/details.aspx?FamilyID=e17e7f31-079a-43a9-bff2-0a110307611e&DisplayLang=en
- For installing a system with Exchange 2003 mail servers, you will require Microsoft Exchange Service Pack 2 for Exchange 2003 System Management Tools, and additional software downloads.
  - Customer-provided Microsoft Exchange System Management Tools. For more information, see Installing third-party software on page 51.

Displaying an MAS from the console

You need to log on as an administrator to the system to access the remote server from the console (monitor). The console is connected to the remote server through the KVM switch.

1. To turn on the S8800 1U server, press the power button on the front of the server, until the LED turns green. For more information, see *Installing the Avaya S8800 Server for Modular Messaging* guide.
2. Verify that the monitor is showing the correct server:
   - For a 2-port Belkin KVM switch, you must connect the MAS to one of the two computer ports.
   - For an 8-port Belkin KVM switch, the first MAS port is labeled **VGA 02**. You must connect the subsequent MASs to the computer ports **VGA 03**, **VGA 04**, and so on.
3. If the monitor displays a different server, toggle the ports to show the correct server:
   - To have a 2-port Belkin KVM switch show a different server:
     a. Gently press **Scroll Lock** twice.

        The LED on top of the Belkin KVM switch starts to blink.

     b. Type the port number on the keyboard. For example, type **2** for port 2.
   - To have an 8-port Belkin KVM switch show a different server:
     a. Gently press **Scroll Lock** twice within 2 seconds.
     b. To display the server, use one of the following methods:
        - Press the up (or down) arrow key to change to the server connected to a higher (or lower) port number.
        - Type the port number on the keyboard. For example, type **2** for port 2.
        - You might see **System Event Log Full** message when the system boots. You can ignore this error message. Modular Messaging does not use this log.

For complete user and troubleshooting instructions, see the KVM switch documentation

Configuring MASs using an existing DCT data file

Use the Avaya Modular Messaging Configuration wizard to access the DCT data file to configure the MAS information automatically.

CAUTION:

Configure each Avaya Messaging Application Server (Avaya MAS) beginning with MAS#1. If you are configuring additional MASs or Supplementary server, use the same data file that you used for MAS#1. *Do not* create a new DCT data file for each MAS or Supplementary server.

1. Verify that you completed the prerequisites before you configure MAS. For more information, see Completing MAS configuration prerequisites on page 46.
2. Make sure that the Peer Exchange server is running.
3. Boot the MAS you want to configure and display it using the console; see Displaying an MAS from the console on page 48.

   When an MAS server boots at this stage of an installation, the Avaya Modular Messaging Configuration wizard runs automatically.
4. Insert the storage device that contains the DCT data file into the server.
5. On the Welcome screen of the **Avaya Modular Messaging Configuration** wizard, click **Next**.
6. On the **Locate Configuration Data** screen, select the appropriate DCT data file for the site. If the required DCT data file is not displayed, click **Browse** and complete the following:
   a. In the **Open** window, click the drop-down list next to **Look in**.
   b. Select the storage device.
   c. Navigate to the appropriate folder on the storage device and double-click the appropriate data file, such as *sitefile*.mmdct.
7. Click **Next**.
8. When the system prompts you to confirm the data file, click **Yes**.

   The wizard opens the Avaya Modular Messaging Data Collection Tool. The DCT executable file (**MMDCT.exe**) launches with the DCT data file that you selected. Review and make any necessary changes to the file.
9. On each DCT window you must do the following:
   a. Verify the data on each screen and click **Next**.

   Note:

   For more information about completing or verifying the data on each screen, see the DCT online help.

b. Under **MM servers**, select **Message store**. The system displays the **Message store screen**.

c. For an Avaya-provided server, if not already selected, select **Microsoft Exchange with Avaya MAS servers**.

d. Click **Complete** to continue the configuration process.

The system prompts you to save the file.

e. You *must* ***Save the file*** even if no changes were made.

CAUTION:

The installation fails if the DCT file is not saved.

The system returns you to the Avaya Modular Messaging Configuration Wizard.

10. On the Messaging Application Server Number screen, specify the **MAS number** field for this server.
    - You *must* configure MAS#1 first.
    - Configure each server in order, including the Supplementary server, if present.
    - If required, change the **MAS number** field to show the correct number for this server.
11. Click **Next**.

    The Configuring System screen shows the progress information of the MAS configuration. The Sysprep window opens. The server then restarts. After the restart, the system runs the Windows Setup wizard.
12. Do the following to complete the wizard:

    a. On the **License Agreement** screen, select **I accept this agreement**. Click **Next**.

    b. On the **Your Product Key** screen, type the Windows product key for this server.
       - Each Windows computer has a unique product key for the Windows 2003 R2 operating system. Enter the exact number.
       - On an S8800 1U server, the product key sticker is located on top of the server chassis.

    c. Click **Next**.

    The Avaya Modular Messaging Configuration Wizard displays the configuration status. During the system configuration, the Avaya Modular Messaging Configuration Wizard restarts the server multiple times and automatically logs on. If during this stage of the installation the automatic logon fails, log on manually to the server as the Modular Messaging Customer Account.

    The Modular Messaging Configuration Wizard pauses at Install Third Party Software dialog.
13. The User Administration Extensions should be installed at this time onto the Messaging Application Server. See Adding the Exchange extensions on page 40.

14. Complete the tasks outlined in Installing third-party software on page 51.

Installing third-party software

To install third party software, perform the following:

- If you are installing third-party software from a mapped network drive, update Windows Internet Explorer 7 security. See Updating Windows Internet Explorer 7 security on page 51.
- For Exchange 2010, see Installing third-party software for Exchange 2010 on page 52
- For Exchange 2007, see Installing third-party software for Exchange 2007 on page 52
- For Exchange 2003, see Installing third-party software for Exchange 2003 on page 53

Updating Windows Internet Explorer 7 security

Note:

When prompted to install third-party software, complete this procedure first if you are installing third-party software from a network drive. If you are installing third-party software from a disc or other removable media, such as a USB memory stick, you can skip this procedure and continue with Installing third-party software on page 51.

Before you install any third-party software, such as antivirus software, you need to update Windows Internet Explorer 7 security. If you do not make this update and you try to use a domain account, such as *custacct*, to install third-party software, Windows does not allow the installation.

1. Launch Windows Internet Explorer 7.
2. A window appears that states Windows Internet Explorer Enhanced Security is enabled; click **OK**.
3. From the browser, select **Tools** > **Internet Options**.
4. From the **Internet Options** window, select the **Security** tab.
5. In the **Select a zone to view or change security settings** box, click **Local intranet**.
6. Click **Sites**.
7. On the **Local intranet** window, click **Advanced**.
8. In the **Add this website to the zone** field, enter any one of the following:
   - *<drive letter>:*\, if you are using a mapped drive,
   - \\<*computername*>\<*share*\, if you are using a fully qualified domain name (FQDN) in the uniform naming convention (UNC) path,
   - the IP address, if you are specifying IP address in the UNC path.

9. Click **Add**.
10. Click **OK** to close the **Local intranet** window.
11. Click **OK** to close the **Internet Options** window.

Installing third-party software for Exchange 2010

Use the procedures in this section to install third-party software when installing Modular Messaging with an Exchange 2010 peer mail server.

When prompted to install third-party software:

1. Install the MAPI Client (v6.5.8190 or later) by double-clicking the MAPI executable file.
2. Install PowerShell 2.0.
3. If you are using Exchange 2007 and Exchange 2010 in a mixed environment, then install Exchange Management Tools for Exchange 2007.
4. Install antivirus software. For more details, see Administering antivirus software on page 54.
5. Complete the MMCW configuration. For details, see Completing the MMCW configuration on page 53.

Installing third-party software for Exchange 2007

Use the procedures in this section to install third-party software when installing Modular Messaging with an Exchange 2007 peer mail server.

When prompted to install third-party software:

1. Install the MAPI Client by double-clicking the MAPI executable file.
2. Install Microsoft Exchange 2007 Management Tools:
   a. Double-click the tools executable file.
   b. Double-click the extracted Microsoft Exchange Installation wizard.
   c. Complete the Microsoft Exchange Installation Wizard selecting **Custom Exchange Server Installation**. Elect to install the **Management Tools**. For details about this procedure, see the Microsoft Exchange documentation.

   You may be prompted to download and install additional components and hotfixes. Follow the installation prompts. Be sure to download the Windows 2003 32-bit version of each component.
3. If prompted, restart the system.
4. Verify that the Exchange Management Tools can communicate with the Exchange 2007 mail server.
5. Follow site-specific procedures to install Microsoft Exchange Server 2007 Service Pack 1.
6. Install antivirus software.see Administering antivirus software on page 54.

7. After installing third-party software, continue with Completing the MMCW configuration on page 53.

Installing third-party software for Exchange 2003

When prompted to install third-party software:

1. Insert the customer-provided Microsoft Exchange 2003 Server media in the MAS drive.
2. Install the Management Tools by completing the Microsoft Exchange Installation Wizard.
3. If you receive a compatibility warning, click **Continue**.
4. For details about this procedure, see the Microsoft Exchange documentation.
5. Install Microsoft Exchange Service Pack 2 and additional software downloads.
6. Installing antivirus software. See Administering antivirus software on page 54.
7. After installing third-party software, continue with Completing the MMCW configuration on page 53

Completing the MMCW configuration

After third-party software is installed, continue with the following steps to complete the configuration.

1. Verify that the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1) in the MAS DVD drive. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8". Click **Continue with installation after installing 3rd-party software** on the 3rd-party dialog box. The MMCW resumes with the following sequence of events:
   - The **Setup** screen displays, followed by the **System Upgrade** screen.
   - The system restarts without user intervention.
   - MMCW restarts automatically and runs the MM Application Setup, installing all MM services.
2. After another restart and auto log on, the MMCW continues the system configuration, displaying informational messages, as each component, such as remote access is configured.
3. When MAS configuration is complete, the progress bar stretches across the window and the Next button becomes active. Click **Next**.
4. On the **Modular Messaging Wizard Completed** screen, click **Finish**.
5. To complete setup of the Modular Messaging server, proceed to Completing the MAS configuration on page 54.

Completing the MAS configuration

To complete the setup of the server complete the following tasks as necessary:

- Administering antivirus software on page 54
- Installing software updates on page 55
- Disabling the private LAN on page 55
- Entering RAS IP addresses on each MAS on page 56
- Continuing the installation on page 57

When you have completed the procedures required for your system, proceed to Configuring the voice mail system on page 79.

Administering antivirus software

Avaya strongly recommends that antivirus software be installed on any Microsoft Windows computer that runs Avaya Modular Messaging software. The type of virus-checking software used and the method of installation depends on customer requirements and the local implementation.

Guidelines for using antivirus software on a computer that is running Avaya Modular Messaging software include:

- Consider the impact that antivirus scanning has on the performance of the Avaya messaging servers. Avaya recommends the use of “on-access” as well as “on-demand” scanning. Avoid using a message-scanning method that could drastically impact the performance of the Avaya servers.

  Note:

  Some antivirus software applications default to scan on startup. Disable this feature, or it increases the time that it takes a system to come back online after a restart.

- Avaya recommends administering the antivirus software as follows:
  - Scan the hard disk at least once per week during off peak hours. Avaya recommends a daily scan. You can run scans on multiple Modular Messaging servers at the same time. However, avoid scheduling the antivirus scan at the same time as when a scheduled backup occurs on the MAS.
  - Schedule virus definition updates to occur automatically at least once per week. The updates must occur before the next scheduled scan time to ensure that the latest data (DAT) files are used during the scan. However, do not schedule updates to occur during a virus scan.

- If the antivirus software locates a virus, it should first attempt to clean the file. If that fails, the software should move the file to a different directory.

Information about antivirus interoperability of Avaya Modular Messaging software with various antivirus products and performance testing is available. The information addresses security issues such as reporting concerns and receiving notifications. For more information, see *antivirus Software on Microsoft Windows-based Avaya Messaging Products.*

Installing software updates

A new Modular Messaging system ships with the most current software that is available at the time. However, the software must be updated after an installation or upgrade to include the latest changes. The updates might be in the form of an Avaya Service Pack (SP) or a software patch (hot fix).

To determine if a Modular Messaging software update is needed:

1. Locate any relevant Avaya software updates on the Avaya Support Web site at http://www.avaya.com/support. For complete steps, see Obtaining software updates from the Web on page 303.

   Note:

   If you followed the procedure for Downloading software updates on page 4, you already downloaded any required software updates.

2. If the Modular Messaging system requires a software update, complete the update procedure now before you do acceptance testing. Follow the instructions in Appendix E: Updating Modular Messaging software on page 303 to update the system with the latest changes.

Disabling the private LAN

The Modular Messaging private LAN is not used with Microsoft Exchange configurations. Disable the private LAN by completing the following steps:

1. On the desktop, right-click the **Network Places** icon. Select **Properties**.
2. In the **Network Connections** window, highlight **IBM USB Remote NDIS Network Device**. Right-click your selection. From the drop-down list, select **disable** to disable the device.
3. In the **Network Connections** window, highlight **Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client) #2**. Right-click your selection. From the drop-down list, select **disable** to disable the device.
4. In the **Network Connections** window, from the toolbar menu, select **Advanced** > **Advanced Settings**. Verify that the corporate LAN is listed at the top of the list of connections. If not, highlight the name of the corporate LAN and use the arrows to move it

up in the list. When finished, close the **Advanced Settings** and **Network Connections** windows.

Entering RAS IP addresses on each MAS

The Avaya Modular Messaging Configuration Wizard automatically sets up inbound remote access to each MAS modem. You must edit the preprogrammed RAS IP addresses to use the addresses that the technical support organization requires.

CAUTION:

If Avaya is to support this system, you must enter the RAS IP addresses assigned by the Avaya Automatic Registration Tool (ART). Otherwise remote access for Avaya technical support will not work.

Complete the following steps for each MAS to set up the IP addresses on MAS to allow remote access:

1. Double-click the **Configure** icon on the desktop.
2. In the left pane of the **Configure** window, expand **Routing and Remote Access**.
3. Expand the server name.
4. Verify authentication:
   a. Highlight **Remote Access Policies**.
   b. On the right pane, double-click **Connections to Microsoft routing and remote access**.
   c. Click the **Edit Profile..** button.
   d. Select the **Authentication** tab.
   e. Make sure that all check boxes (except for the **Unauthenticated access** check box) are selected. If necessary, clear the **Unauthenticated access** check box.
   f. Click **OK**.
   g. If a dialog box appears, click **No**.
   h. Click **OK**.
5. Right-click the server name from the pop-up menu and select **Properties**.
6. Set up PAP security:
   a. In the **Local Properties** window, click the **Security** tab.
   b. Click **Authentication Methods...**
   c. Select **Unencrypted Password (PAP)**.
   d. Verify that all other check boxes are blank. If necessary, clear the check boxes.
   e. Click **OK**.

7. Set up a static IP address pool as follows:
   a. In the local **Properties** window, click the **IP** tab.
   b. Under **IP address assignment**, select **Static address pool**.
   c. Add or edit the address range as follows:
      - If the window shows an incorrect IP address range, select the displayed range and click **Edit**.

      CAUTION:
      If Avaya Modular Messaging is to support this MAS, do not use the preprogrammed IP addresses. You must Edit and Remove these addresses for remote access to work.

      - If no address range is already entered, click **Add**.
   d. In the **Address Range** dialog box, enter the correct start and end IP addresses for this server.To get the start and end IP addresses, you *must* register your system.
   e. Verify that the number of addresses is **2**.
   f. Click **OK**.
   g. In the **Adapter** field, select **Allow RAS to select adapter**.
   h. Click **OK** to close the **Properties** window.
   i. If a dialog box appears, click **No**.
   j. Close the **Configure** window.

Continuing the installation

When you have finished installing the MAS, you must continue with configuring the voice mail system. See Configuring the voice mail system on page 79.

Chapter 5: Configuring a customer-provided MAS

This chapter applies only to a customer-provided Messaging Application Server and supplementary server installation. This chapter describes Modular Messaging MAS installation on a customer-provided hardware.

If you are installing an S8800 1U server, do not use the procedures in this chapter. See Chapter 4: Configuring an Avaya MAS on page 45.

CAUTION:

Before you can proceed with the tasks described in this section, a system administrator must have successfully completed the tasks in Chapter 2: Preparing to install Modular Messaging software on page 9.

Important:

Customer-provided equipment (CPE) for a Modular Messaging install or upgrade must match the specifications described in *Avaya Modular Messaging Concepts and Planning Guide*.

Obtain the current DCT data file for this site before you configure the customer-provided MAS. A person responsible for planning the installation creates the file using the Modular Messaging Data Collection Tool (DCT) before the Modular Messaging system is installed. The DCT data file has an extension **mmdct**, such as *sitefile.mmdct*. For more information, see *Data Collection Tool* guide.

Topics in this chapter include:

- Customer-provided MAS configuration prerequisites on page 60
- Preparing the customer-provided MAS on page 61
- Configuring the customer-provided MAS on page 68
- Completing the customer-provided MAS configuration on page 74

Customer-provided MAS configuration prerequisites

You can use a customer-provided server to support Modular Messaging software. However, you must first configure the server to support Modular Messaging in a Microsoft Exchange environment.

The majority of the Modular Messaging server configuration is completed by the Modular Messaging Configuration Wizard (MMCW). The MMCW configures the MAS from information in a site-specific configuration file called a Data Collection Tool (DCT) data file (**.mmdct*). This file is created using the DCT executable file (**MMDCT.exe**). Typically the DCT data file (*.mmdct) is created prior to the installation by the project manager, customer administrator and other experts responsible for the installation.

See the DCT online help system or its printed version, *Avaya Modular Messaging Data Collection Tool Help*, for a complete description of the procedure and specifications for creating a DCT data file.

Note:

Always check the Avaya Support Web site at http://www.avaya.com/support for recent updates to the DCT executable file (MMDCT.exe).

To successfully set up a customer-provided server, you need:

- A complete and valid DCT data file.
- A printout of the customer-provided MAS installation checklist. See New Modular Messaging installation on a customer-provided MAS on page 230. Check off steps as you complete them to track your progress.
- The following software from the Avaya Support Web site at http://www.avaya.com/support. For more information about how to access these items on the Web site, see Downloading required software and documentation on page 3.
  - Avaya software updates that are required to bring the Modular Messaging software up to date after an installation. Download this software to a USB storage device. For more information about downloading the updates, see Updating Modular Messaging software on page 303.
  - The latest copy of the DCT executable file (**MMDCT.exe**). Download the file from the Avaya support Web site to a USB storage device. Download the executable file to the same USB storage device as the DCT data file.
  - Modular Messaging Outlook Thick Client (OTC).
- WebLM server installable, if you choose to install the WebLM on a standalone server. For instructions, see *Installing and configuring Avaya WebLM server*.
- The latest Modular Messaging license file obtained and applied on the WebLM server, if you are installing WebLM on a standalone server or using an existing WebLM server, For more information, see:

- Obtaining the license file on page 91
- Applying license file on the WebLM server on page 91

- To install a MAS with Exchange 2010 mail servers, you need:
  - MAPI Client v6.5.8190 or later
  - Microsoft Management Console 3.0
  - .NET 3.5 SP1
  - PowerShell 2.0
- For installing a system with Exchange 2007 mail servers, you require the 32-bit version of the Exchange 2007 Management Tools and Microsoft Exchange 2007 Service Pack 1. You may download the 32-bit version of the Exchange 2007 Management Tools from:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=444C259E-605F-4A82-96D5-A2F448C9D4FF&displaylang=en
- For installing a system with Exchange 2003 mail servers, you require Microsoft Exchange 2003 Service Pack 2 and Exchange 2003 Management Tools.
  - Customer-provided Microsoft Exchange System Management Tools from the customers Exchange administrator. For more information, see Installing third-party software on page 71.
- Microsoft Windows 2003 Service Pack 2 if the Service Pack has not been installed on the system.

Preparing the customer-provided MAS

Complete the following procedures to set up this customer-provided server to support Avaya Modular Messaging services.

- Installing Microsoft Windows 2003 R2 operating system on page 62
- Running recommended disk checks on page 62
- Installing modem drivers on the customer-provided MAS on page 62
- Adjusting system values on page 62
- Installing and enabling Microsoft Windows services on page 64
- Installing Microsoft Windows 2003 SP2 on page 66
- Installing Microsoft Windows updates and security patches on page 66
- Joining the Windows domain on page 67
- Adding Modular Messaging accounts to the local administrators group on page 68

Installing Microsoft Windows 2003 R2 operating system

Avaya recommends that you complete a new installation of Windows 2003 R2, when you perform new installations of Modular Messaging with CPE hardware. While installing Windows 2003 R2, ensure that you *only* install the Windows services listed in Installing and enabling Microsoft Windows services on page 64.

Setting a computer name

When installing Windows 2003 R2 on the server, provide a name to the computer.

When you run the Modular Messaging Configuration Wizard, the system does not automatically change the name of the computer as in an Avaya-provided MAS. You must manually provide the name of the computer before you run the Modular Messaging Configuration wizard.

Running recommended disk checks

Perform this procedure only for a supplementary server.

Avaya recommends that the hard disk drive in the server be maintained to prevent possible problems. The system administrator must run the following on a regular basis:

- Disk Defragmenter system tool
- **chkdsk** command

If this server is in service and has not been recently maintained, run the two recommended procedures.

Installing modem drivers on the customer-provided MAS

For customer-provided MAS, the customer must install the drivers for serial adapters, serial port and the modem. Avaya does not take the responsibility of installing modems on the customer-provided MAS.

Adjusting system values

You must adjust some default values on the server to support Modular Messaging. Verify the following settings, and adjust them if needed:

1. Adjust the values for the Event Viewer:
   a. Right-click **My Computer** and select **Manage**.

b. In the **Computer Management** window, in the left pane, expand **Event Viewer**.

c. Adjust the application log values:

1. Right-click **Application** and select **Properties**.
2. On the **General** tab of the **Application Properties** window, under **Log size**, adjust the following values:
   - Avaya recommends that you set **Maximum log size** to at least 102400 KB.
   - Select **Overwrite events as needed**.
3. Click **OK** to close this window.

d. Adjust the system log values:

1. In the right pane, right-click **System** and select **Properties**.
2. On the **General** tab of the **System Properties** window, under **Log size**, adjust the following values:
   - Set **Maximum log size** to at least 4032 KB.
   - Select **Overwrite events as needed**.
3. Click **OK** to close this window.

e. Close the **Computer Management** window.

2. Right-click **Start** and select **Explore**. Adjust File and Printer Sharing properties:

a. Right-click **My Network Places** and select **Properties**.

b. Right-click **Local Area Connection** and click **Properties**.

c. Select **File and Printer Sharing for Microsoft Networks** in the list box and click **Properties**.

d. On the **Server Optimization** tab, select **Maximize data throughput for network applications**.

e. Click **OK** to close this window.

f. Close the **Local Area Connection Properties** and **Network Connections** windows.

3. Adjust the Windows Server 2003 operating system values:

a. Right-click **My Computer** and select **Properties**.

b. Click the **Advanced** tab.

c. Under **Performance**, click **Settings**.

d. In the **Performance Options** window, click the **Advanced** tab.

1. Under **Processor Scheduling**, select **Background services**.
2. Under **Virtual memory**, click **Change**.

3. The **Initial size** and **Maximum size** fields for the **Paging file size for selected drive** value vary by machine. Tailor these fields by adding 11 to the default value that is displayed as follows:
   - Under **Paging file size for selected drive**, set both the **Initial size** and **Maximum size** to the default value plus **11** MB.
   - Click **Set**.
   - Click **OK** to close this window.
4. Click **OK** to close the **Performance Options** window.

e. On the **Advanced** tab of the **System Properties** window, under **Startup and Recovery**, click **Settings**.

f. In the **Startup and Recovery** window, under **System Failure**, verify that the check box to **Automatically restart** is checked. Click **OK**.

g. Click **OK** to close this window.

4. Restart the server before continuing:
   - If you are prompted to restart the server, click **Yes**.
   - If the system does not prompt you, manually restart the server now. For example:
     a. Press **Ctrl**+**Alt**+**Del**, and then click **Shut Down**.
     b. Select **Restart** from the drop-down list and click **OK**.

   The server restarts.

Installing and enabling Microsoft Windows services

You must install and enable the Microsoft Windows services on each customer-provided MAS that handles voice calls as described in this section.

To install and enable all required Windows services:

1. Log on to an account that has permissions to install software on this computer, such as the local administrator account.
2. Remove any external hard drives from the MAS.
3. Insert the Microsoft Windows Operating System CD in the MAS drive.
4. Click **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.
5. In the **Add or Remove Programs** window, in the left column, click **Add/Remove Windows Components**.
6. To install Microsoft Windows services:
   a. In the **Windows Components Wizard** window, highlight **Application Server**. Click **Details**.

b. Verify that the following items are checked:

- Application Server Console
- ASP.NET
- Enable COM+ access
- Message Queuing

The **Internet Information Services (IIS)** checkbox becomes checked.

c. Highlight **Internet Information Services (IIS)**. Click **Details**. Verify that the following items are checked:

- Common Files
- Internet Information Services Manager
- World Wide Web Server

Note:

When you check these items, IIS gets checked automatically.

The Internet Information Services items listed above are always required.

If you plan to install the Microsoft Exchange 2003 System Management Tools, click the checkboxes for **NNTP Service** and **SMTP Service**. The SMTP Service automatically selects other required components as needed.

If you plan to install the Microsoft Exchange 2007 Management Tools, do *not* install NNTP Service and SMTP Service.

If you plan to install an MAS with the Microsoft Exchange 2010 mail server, do not install NNTP Service and SMTP Service.

d. In the same window, highlight **World Wide Web Server** and click **Details**. Verify that World Wide Web Services is checked.

e. Close this and the next two windows.

7. Install the Windows services to support SNMP:

a. in the **Windows Components Wizard** window, highlight **Management and Monitoring Tools** and click **Details**.

b. Click the checkbox to select **Simple Network Management Protocol** and click **OK**.

8. Install the Windows Fax Service, in the **Windows Components Wizard** window:

a. Check **Fax Services**. Click **Next**.

b. Select **Do Not Share Fax Printer** and click **Next**.

9. Complete the wizard to install the selected services.

Note:

If the required services were already installed (all the appropriate boxes were checked), click **Cancel** to close the wizard.

10. When the installation is complete, close the **Add or Remove Programs** window.
11. After the software is installed, enable each installed service as follows:
    a. Right-click **My Computer** and select **Manage**.
    b. In the left (Tree) pane, expand **Services and Applications**, and click **Services**.
    c. In the right pane, scroll down to the first new service that you installed. Double-click the service.
    d. In the **Properties** window:
        1. On the **General** tab, set the **Startup type** to **Automatic**. Click **Apply**.
        2. Under **Service status**, click **Start**.
        3. Wait for service to start, and then click **OK** to close this window.
    e. Repeat Steps c and d to enable each of the services you installed. Note that only a subset of these services might be present on a particular MAS.
12. When all services are enabled, close all open windows.

Installing Microsoft Windows 2003 SP2

Verify the Windows service pack version on each customer-provided MAS and install Windows 2003 SP2 if it is not installed.

Complete the following to verify the version of the service pack installed:

1. Right-click **My Computer** and select **Explore**.
    a. In Windows Explorer, click **Help** > **About Windows**.
    b. In the version description, verify that Microsoft Windows Service Pack 2 is installed.
    c. Click **OK** to close this window.
    d. Close Windows Explorer window.
2. If needed, install Microsoft Windows Service Pack 2 on this MAS.

Installing Microsoft Windows updates and security patches

You must install the latest Microsoft Windows software, 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.

Avaya technical support representatives must follow the specified internal procedures to verify the software that is installed. If required, the support representative must update the software with the latest patches as instructed.

Joining the Windows domain

You must manually add this server to the appropriate Windows domain for this Modular Messaging system:

1. Switch the monitor to show this server.

   Use whatever method is required at this site to have the monitor display the MAS that you are administering.

2. Log on to the local administrator account for this server:

   a. In the **Log On to Windows** window, change the user name to the local administrator account name.

   b. Enter the password for this account.

   c. If the **Log in to:** field shows a different domain, use the drop-down box to select this server.

   d. Press **Enter** or click **OK**.

3. Right-click **My Computer** and select **Properties**.

4. In the **System Properties** window:

   a. Click the **Computer Name** tab.

   b. Click **Change**.

5. In the **Computer Name Changes** window:

   a. Under **Member of**, select **Domain**.

   b. Type the name for the corporate Windows domain.

   Note:

   Depending on the local configuration, you might need to enter the fully qualified name here.

   c. Click **OK**.

   d. Another **Computer Name Changes** window might open. If it does:

      1. Enter the name of an account that has permissions to join the Windows domain. You usually use the Modular Messaging customer account, if the domain administrator has set up the account as described in Creating Modular Messaging customer and

technical support accounts on page 10. The account name must be in the format ***domain\account name***, such as *domain1\mmacct*.

2. Enter the password for this account. Click **OK**.

6. If a Welcome to the domain message is displayed, click **OK**.
7. When prompted to restart, click **OK**.
8. Click **OK** to close the **System Properties** window.
9. If you are prompted to restart the server, click **Yes.**

Adding Modular Messaging accounts to the local administrators group

For the accounts to work correctly, you must add the Modular Messaging customer account and the technical support account to the local administrators group:

1. Log on to the local administrator account for this server.
2. Click **Start** > **Control Panel**.
3. Double-click **Administrative Tools**.
4. Double-click **Computer Management**.
5. Under **System Tools**, expand **Local Users and Groups**, and then click **Groups**.
6. Double-click the **Administrators** group in the right pane.
7. In the **Administrators Properties** window, click **Add**.
8. In the **Enter object names to select** pane, enter the names of the customer account and technical support remote access account. The account names must be in the format ***domain\account name*** (such as *domain1\mmacct*).

   Note:

   You can search for the accounts by entering a portion of the name in the **Enter the object names to select** pane, and clicking **Check Names**.

   After names are entered, click **OK**.
9. Click **OK** to close this window.
10. Close the **Computer Management** and **Administrative Tools** windows.

Configuring the customer-provided MAS

Before you use the updated DCT data file and run the Avaya Modular Messaging Configuration

wizard to configure the server, you must complete the following procedures.

- Obtain the latest ***MMDCT.exe*** file. For details, see Downloading software updates on page 4.
- Obtain the required DCT data file (***.mmdct***).
- Ensure that the DCT file is accessible to the server that you install. Usually, this means inserting a storage device with the file into the server.

Running the Modular Messaging Configuration wizard

The Modular Messaging Configuration wizard (MMCW) uses the DCT data file to configure the customer-provided MAS. You must install the Modular Messaging Configuration wizard (MMCW) to configure each customer-provided MAS.

Complete the following to configure the customer-provided MAS server using Modular Messaging DCT:

1. Verify that the USB storage device with the DCT data file (*.mmdct) and most recent DCT executable file (**MMDCT.exe**) is inserted in the USB port.
2. Turn the server on.
3. Log on to the MAS using the Modular Messaging customer account created in Creating Modular Messaging customer and technical support accounts on page 10.
4. Insert the 'Avaya Modular Messaging R5.2 MAS Application DVD 1 of 2' disk into the DVD drive of the customer-provided MAS server. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
5. Navigate to the ***Install\MISCM*** directory and double-click the ***MMConfigurationWizard.msi*** file.

   The system installs the configuration wizard in the ***C:\Program Files\Avaya Modular Messaging\Install\MISCM*** directory and launches the Modular Messaging configuration wizard.
6. Click **Finish**.

   The system opens the **Modular Messaging DCT Tool** window.
7. On the **Modular Messaging Welcome** screen, click **Next**.
8. On the **Locate Configuration Data** screen, click **Browse**.
   a. In the **Open** window, click the drop-down list next to **Look in**.
   b. Navigate to the storage device.

      If the server fails to recognize the storage device, you can:

      1. In the Open window, click **My Computer** in the left pane. After the **Look in** field shows **My Computer**, press **F5** to refresh the screen.

2. If the system fails to display the storage device, unplug the device and insert the device again.

c. Double-click the most current DCT data file.

9. On the **Locate Configuration Data** screen, click **Next**.
10. When the system prompts you to confirm the data file, click **Yes**.

    The system opens Avaya Modular Messaging Data Collection Tool window.
11. On each DCT window you must do the following:

    a. Verify the data on each screen and click **Next**.

    Note:

    For more information about completing or verifying the data on each screen, see the DCT online help.

    b. Under **MM servers**, select **Message store**. The system displays the **Message store screen**.

    c. For a customer-provided server, if not already selected, select **Microsoft Exchange with customer's MAS servers**.

    d. Click **Complete** to continue the configuration process.

    The system prompts you to save the file.

    e. You *must* ***Save the file*** even if no changes were made.

    CAUTION:

    The installation does not complete successfully if the DCT file is not saved.

    The system returns you to the Avaya Modular Messaging Configuration Wizard.

    Note:

    Do not click **Cancel**, as this may result in a need for a re-install of the system.
12. On the **Messaging Application Server Number** screen, specify the **MAS number** field to show the correct number for this server.
13. Click **Next**.
14. When the system prompts you to log on, log on to the customer-provided MAS using the customer account.
15. When the configuration wizard prompts you to locate the ***InstallRSEngine.bat*** file, insert the 'Modular Messaging R5.2 MAS Application DVD 2 of 2' disk. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
16. When you receive the error message that the **<drive>:\Realspeak** location is not available:

    a. Click **OK** to close the dialog box.

    b. In the **Look In** field, click **Browse** to choose the DVD drive and double-click the **Realspeak** directory.

c. Double click on the **realspeakengine.bat** file.

The **RealSpeak 4.0 InstallShield** wizard starts.

17. If you are installing Modular Messaging to the default **C:** drive, complete the wizard by accepting all default values. If you are installing Modular Messaging to an alternate drive, complete the following steps:

    a. Move through the RealSpeak installation wizard accepting defaults until you see the **Custom Setup** screen.

    b. On the **Custom Setup** screen, highlight RealSpeak Common Components. Click the arrow next to **RealSpeak Common Components** and select **This feature and all subfeatures will be installed on local hard drive**. Click **Change**.

    c. On the **Change Current Destination Folder** screen, in the **Folder name:** field change the letter of the drive to match the drive where Modular Messaging is being installed. This drive is set in the DCT data file. Do not browse to find the new location. The path will read ***<drive letter>*:\Program Files\ScanSoft\RealSpeak 4.0**.

    d. Click **OK** and continue to accept default values to complete the wizard.

18. After the RealSpeak engine is installed, at the prompt to restart the system, choose to restart.
19. After the system restarts, log on using the customer account, for example *mmacct*. The RealSpeak languages install.
20. Click **Next**.

    The Avaya Modular Messaging Configuration Wizard displays the configuration status. During the system configuration, the Avaya Modular Messaging Configuration Wizard restarts the server multiple times and automatically logs on.

    The Modular Messaging Configuration Wizard pauses at Install Third Party Software dialog.

21. The User Administration Extensions should be installed at this time onto the Messaging Application Server. See Adding the Exchange extensions on page 40.
22. Complete the tasks outlined in Installing third-party software on page 71.

Installing third-party software

To install third party software, perform the following:

- If you are installing third-party software from a mapped network drive, update Windows Internet Explorer 7 security. See Updating Windows Internet Explorer 7 security on page 72.
- For Exchange 2010, see Installing third-party software for Exchange 2010 on page 72.
- For Exchange 2007, see Installing third-party software for Exchange 2007 on page 73
- For Exchange 2003, see Installing third-party software for Exchange 2003 on page 73

Updating Windows Internet Explorer 7 security

Note:

When prompted to install third-party software, complete this procedure first if you are installing third-party software from a network drive. If you are installing third-party software from a disc or other removable media, such as a USB memory stick, you can skip this procedure and continue with Installing third-party software on page 71.

Before you install any third-party software, such as antivirus software, you need to update Windows Internet Explorer 7 security. If you do not make this update and you try to use a domain account, such as *custacct*, to install third-party software, Windows does not allow the installation.

1. Launch Windows Internet Explorer 7.
2. A window appears that states Windows Internet Explorer Enhanced Security is enabled; click **OK**.
3. From the browser, select **Tools** > **Internet Options**.
4. From the **Internet Options** window, select the **Security** tab.
5. In the **Select a zone to view or change security settings** box, click **Local intranet**.
6. Click **Sites**.
7. On the **Local intranet** window, click **Advanced**.
8. In the **Add this website to the zone** field, enter any one of the following:
   - *<drive letter>:*\, if you are using a mapped drive,
   - \\<*computername*>\<*share*\, if you are using a fully qualified domain name (FQDN) in the uniform naming convention (UNC) path,
   - the IP address, if you are specifying IP address in the UNC path.
9. Click **Add**.
10. Click **OK** to close the **Local intranet** window.
11. Click **OK** to close the **Internet Options** window.

Installing third-party software for Exchange 2010

Use the procedures in this section to install third-party software when installing Modular Messaging with an Exchange 2010 peer mail server.

When prompted to install third-party software:

1. Install the MAPI Client (v6.5.8190 or later) by double-clicking the MAPI executable file.
2. Install PowerShell 2.0.

3. If you are using Exchange 2007 and Exchange 2010 in a mixed environment, then install Exchange Management Tools for Exchange 2007.
4. Install antivirus software. For more details, see Administering antivirus software on page 54.
5. Complete the MMCW configuration. For details, see Completing the MMCW configuration on page 74.

Installing third-party software for Exchange 2007

Use the procedures in this section to install third-party software when installing Modular Messaging with an Exchange 2007 peer mail server.

When prompted to install third-party software:

1. Install the MAPI Client by double-clicking the MAPI executable file.
2. Install Microsoft Exchange 2007 Management Tools:
   a. Double-click the tools executable file.
   b. Double-click the extracted Microsoft Exchange Installation wizard.
   c. Complete the Microsoft Exchange Installation Wizard selecting **Custom Exchange Server Installation**. Elect to install the **Management Tools**. For details about this procedure, see the Microsoft Exchange documentation.

   You may be prompted to download and install additional components and hotfixes. Follow the installation prompts. Be sure to download the Windows 2003 32-bit version of each component.
3. If prompted, restart the system.
4. Verify that the Exchange Management Tools can communicate with the Exchange 2007 mail server.
5. Follow site-specific procedures to install Microsoft Exchange Server 2007 Service Pack 1.
6. Install antivirus software.see Administering antivirus software on page 54.
7. After installing third-party software, continue with Completing the MMCW configuration on page 74.

Installing third-party software for Exchange 2003

When prompted to install third-party software:

1. Insert the customer-provided Microsoft Exchange Server media in the MAS drive.
2. Install the Management Tools by completing the Microsoft Exchange Installation Wizard.
3. If you receive a compatibility warning, click **Continue**.
4. For details about this procedure, see the Microsoft Exchange documentation.
5. Install Microsoft Exchange Service Pack 2 and additional software downloads.

6. Installing antivirus software. See Administering antivirus software on page 54.
7. After installing third-party software, continue with Completing the MMCW configuration on page 74.

Completing the MMCW configuration

After third-party software is installed, continue with the following steps to complete the configuration:

1. Verify that the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1) in the MAS DVD drive. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8". Click **Continue with installation after installing 3rd-party software** on the 3rd-party dialog box. The MMCW resumes with the following sequence of events:
   - The **Setup** screen displays, followed by the **System Upgrade** screen.
   - The system restarts without user intervention.
   - MMCW restarts automatically and runs the MM Application Setup, installing all MM services.
2. After another restart and auto log on, the MMCW continues the system configuration, displaying informational messages, as each component, such as remote access is configured.
3. When MAS configuration is complete, the progress bar stretches across the window and the Next button becomes active. Click **Next**.
4. On the **Modular Messaging Wizard Completed** screen, click **Finish**.
5. To complete setup of the Modular Messaging server, proceed to Completing the customer-provided MAS configuration on page 74.

Completing the customer-provided MAS configuration

Perform the following tasks to complete the configuration of the customer-provided MAS:

- Installing software updates on page 75
- Verifying default LAN name and Power Management settings on page 75
- Entering the RAS IP addresses on customer-provided MAS on page 76
- Setting logging location on page 77
- Continuing the installation on page 78

Installing software updates

A new Modular Messaging system ships with the most current software that is available at the time. However, the software must be updated after an installation or upgrade to include the latest changes. The updates might be in the form of an Avaya Service Pack (SP) or a software patch (hot fix).

To determine if a Modular Messaging software update is needed:

1. Locate any relevant Avaya software updates on the Avaya Support Web site at http://www.avaya.com/support. For complete steps, see Obtaining software updates from the Web on page 303.

   Note:

   If you followed the procedure for Downloading software updates on page 4, you already downloaded any required software updates.

2. If the Modular Messaging system requires a software update, complete the update procedure now before you do acceptance testing. Follow the instructions in Appendix E: Updating Modular Messaging software on page 303 to update the system with the latest changes.

Verifying default LAN name and Power Management settings

Rename the corporate LAN connection for this MAS so that it is easier to identify. To rename the LAN entry:

1. . Click **Start > Settings > Network Connections**.

   The **Network Connections** window opens.

2. Identify the corporate LAN on this server. The corporate LAN is labelled **Local Area Connection**.

   Rename this item as follows:

   a. Right-click the text **Local Area Connection** and select **Rename**.

   b. Change the name to **Corporate LAN**.

3. Change the Power Management settings for the LAN connection:

   a. Right-click the LAN connection and select **Properties**.

   b. Click **Configure**.

   c. Click the **Power Management** tab.

   d. Deselect the **Allow the computer to turn off this device to save power** checkbox.

4. Close any LAN-connection windows.

Entering the RAS IP addresses on customer-provided MAS

Remote access allows technical support staff to dial into a system to correct problems and perform routine maintenance. You must provide a method for remote services to access the system. Follow site-specific requirements to set up remote access or complete the following procedure.

The Avaya Modular Messaging Configuration Wizard automatically sets up inbound remote access to each MAS modem. You must edit the preprogrammed RAS IP addresses to use the correct addresses that the technical support organization requires.

CAUTION:

If Avaya is to support this system, you must enter the RAS IP addresses assigned by the Avaya Automatic Registration Tool (ART). Otherwise remote access for Avaya technical support will not work.

To set up IP addresses on each MAS to allow remote access:

1. Double-click the **Configure** icon on the desktop.
2. In the left pane, expand **Routing and Remote Access**.
3. Expand the server name.
4. Verify authentication:
   a. Highlight **Remote Access Policies**.
   b. From the right pane, double-click **Connections to Microsoft routing and remote access**.
   c. Click the **Edit Profile..** button.
   d. Select the **Authentication** tab.
   e. Verify that all check boxes (except for the **Unauthenticated access** check box) are selected. If necessary, clear the **Unauthenticated access** check box.
   f. Click **OK**.
   g. If a dialog box appears, click **No**.
   h. Click **OK** again.
5. Right-click the server name from the pop-up menu and select **Properties**.
6. Set up PAP security:
   a. In the **Local Properties** window, click the **Security** tab.
   b. Click **Authentication Methods...**
   c. Select **Unencrypted Password (PAP)**.
   d. Verify that all other check boxes are blank. If necessary, clear the check boxes.

e. Click **OK**.

7. Set up a static IP address pool as follows:
   a. In the **Local Properties** window, click the **IP** tab.
   b. Under **IP address assignment**, select **Static address pool**.
   c. Add or edit the address range as follows:
      - If the window shows an incorrect IP address range, select the displayed range and click **Edit**.

      CAUTION:
      If Avaya will support this server, do not use the preprogrammed IP addresses. You must Edit and Remove these addresses for remote access to work.

      - If no address range is already entered, click **Add**.
   d. In the **Address Range** window, enter the correct start and end IP addresses for this server.
   e. Verify that the number of addresses is **2**.
   f. Click **OK**.
   g. For the **Adapter** field, select **Allow RAS to select adapter**.
   h. Click **OK** to close the properties window.
   i. If a dialog box appears, click **No**.
   j. Close the **Configure** window.

Setting logging location

CAUTION:
You must have adequate space on the drive where your logs are located. If you do not, your system may fail to operate correctly. Check the location where your system is recording logs to be sure you don't overrun your allotted space.

You may want to change the default location for recording logs if you do not have adequate space on the default **C:** drive location. Likewise, if you installed Modular Messaging to a drive other than the default **C:** drive, the logging location is not automatically changed. In this case you may want to change the location for recording logs to the same drive as the software installation.

To change the location for recording logs, complete the following steps:

1. Navigate to the following location on the drive where Modular Messaging was installed: **<*drive letter*>:\Avaya_Support\Tools**

2. Double-click the **MM_Logging.exe** file.

   The Modular Messaging **Verbose Logging** Window opens.

3. Complete the following steps for each type of log displayed at the top of the screen with the exception of the **Client**.

   a. Click the log-type button.

   b. In the **Folder for Log Files:** field, edit the drive letter to the drive where you want logs stored. If you have installed Modular Messaging to an alternate drive, edit the field to show the drive where Modular Messaging was installed.

   c. Click **Apply** at the bottom of the screen.

4. When the log location has been changed for all log types, click **Close** at the bottom of the screen.

The MM Debug Log Viewer should be set up to open log files automatically after installation. If for some reason this association is not made or it becomes changed, do the following manual setup.

To manually set up MM Debug Log Viewer:

1. From the desktop, open **My Documents** (or any Windows Explorer window).
2. Click **Tools > Folder Options > File Types**.
3. Is LOG4 listed in the extensions list?
   - If YES, skip to step 7.
   - If NO, continue with step 4.
4. Click **New**.
5. In the **Create New Extension** box, type **log4**. Click **OK**.
6. In the extensions list, at the top, highlight **LOG4**. Click **Change**.
7. Click **Select the program from a list**.
8. In the **Open With** window, highlight **MM Debug Log Viewer**. If that selection is not present, click **Browse** and navigate to and select **C:\AVAYA_Support\Tools\LogViewer\MMLogViewer.exe**.
9. Click **OK**.
10. Close all windows.

Continuing the installation

When you have finished installing the MAS, you must continue with configuring the voice mail system. See Configuring the voice mail system on page 79.

Chapter 6: Configuring the voice mail system

This chapter describes how to configure the basic Voice Mail System Configuration (VMSC) parameters and complete initial Modular Messaging software administration.

Note:

For new installations: Before you can complete the tasks described in this section, you must have completed the tasks in Chapter 4: Configuring an Avaya MAS on page 45 or Chapter 5: Configuring a customer-provided MAS on page 59.

For upgrades: Before you can complete the tasks described in this section, you need to complete the tasks either in Chapter 8: Upgrading Modular Messaging software on an Avaya MAS on page 123 or Chapter 9: Upgrading Modular Messaging software on a customer-provided server on page 145.

For migrations: Before you can complete the tasks described in this section, you need to complete the tasks either in Migrating to Modular Messaging Release 5.2 on an Avaya MAS on page 169 or Migrating to Modular Messaging Release 5.2 on a customer-provided server on page 193.

Additionally, if port boards are installed on the MAS and are not automatically configured by the Modular Messaging Configuration Wizard (MMCW) you must complete the tasks in Appendix F: Configuring and testing port boards on page 307 before configuring the voice mail system. See When to configure port boards on page 307 for a list of automatically configured integrations.

Important:

New installations of Modular Messaging support:

- SAL alarming and remote access *only.*
- SIP based switch integration *only*.

Configuring the voice mail system

Voice mail system can be classified, as follows:

1. Domain-wide administration that must be done once for each new installation. You usually do these procedures on MAS#1, although you can adjust them later if needed.
2. Administration of domain-wide features that can be installed on any MAS, such as Call Me or Message Waiting Indicator (MWI).

3. Configuration information specific to each MAS, such as INADS alarming or port board administration.

This section describes how to configure key parameters to make the new system operational. Complete the tasks in this section to get the Modular Messaging system up and running with the basic required features. After the installation is complete, Avaya encourages customers to tailor the Voice Mail System Configuration (VMSC) parameters for their site. For more information, see the *Avaya Modular Messaging MAS Administration Guide*.

CAUTION:

You can complete some procedures in this section only if you use the required configuration notes for a specific PBX. For instructions to obtain the configuration notes, see Downloading configuration notes on page 4.

Topics in this chapter include:

- Configuring required domain-wide features on page 80
- Installing and configuring the WebLM server on an MAS on page 89
- Obtaining the license file on page 91
- Applying license file on the WebLM server on page 91
- Entering Product ID for current MAS on page 93
- Configuring specific features as needed on page 93
- Configuring MAS-specific parameters on page 99
- Restarting messaging services on page 102
- Verifying basic operation of this MAS on page 104
- Continuing the installation on page 106

Configuring required domain-wide features

This section describes how to configure domain-wide features that are required for each Modular Messaging system. Required features are:

- Specifying languages on page 81
- Verifying that Modular Messaging service has started on MAS#1 on page 81
- Configuring TUI and access settings on page 82
- Configuring the broadcast mailbox on page 83
- Configuring the PBX type on page 86
- Configuring serviceability settings on page 86

- Installing WebLM server on an MAS on page 90
- Obtaining the license file on page 91

For a new installation, do these procedures on the first MAS that is installed to ensure the configuration of all required system features.

For information on MultiSite concepts and requirements, see *Modular Messaging MultiSite Guide*. For MultiSite specific configuration, see the **Voice Mail System Configuration** section in *Avaya Modular Messaging MAS Administration Guide*.

Specifying languages

Important:

If you change the language settings of the Modular Messaging system, the change only affects the display language for applications and tools on the Modular Messaging system, and does not impact TUI prompting languages. To configure the TUI languages, see *Avaya Modular Messaging MAS Administration Guide*. If you change the language of the Modular Messaging system, be sure to also change the language settings for Windows. (See Windows documentation for this information).

Specify the preferred language for this MAS if the Windows operating system is set to a non-English language:

1. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Languages**.
2. In the **Modular Messaging User Properties** window, select the **Preferred language** from the drop-down list.
3. Click **OK** to close this window.

Verifying that Modular Messaging service has started on MAS#1

Verify if Modular Messaging service has started before you configure the voice mail system.

1. Right-click **My Computer** and select **Manage**. In the **Computer Management** window, the left (Tree) pane, expand **Services and Applications**.
2. Click **Services (Local)** in the left pane, if the item is not already selected.
3. In the right pane, scroll down to **MM Messaging Application Server**.
4. Check the **Status** column, if the status is **Started**, close the **Monitor** window and proceed with the steps in Configuring TUI and access settings on page 82.
5. If the Modular Messaging service has *not* started, right-click **MM Messaging Application Server** and select **Start**.

   The system starts the messaging service. When you restart the messaging service, the **Monitor** window immediately displays status as **Started**. However, the service might

actually take several minutes to start. The time taken to start the service depends on the number of port boards installed and the integration method used.

6. Expand the **Event Viewer (Local)** in the left pane to track the progress in startup. Click **Application**.
7. Refresh the **Monitor** window until you see Telephony User Interface event 1241, **TUI service has been enabled**.
8. Verify if MM Service Connector service has also started. If the Service Connector has not started, right-click **MM Service Connector** and select **Start**
9. Minimize the **Monitor** window. You will use it later.

Configuring TUI and access settings

You must configure the settings in this section once for each Modular Messaging system (VMD).

1. Click **Start > Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration**.

   The **Voice Mail System Configuration** window opens. All MASs present in the messaging system are listed under the voice mail domain.

   Note:

   Do the steps in this section for entries under the voice mail domain, such as *vmdom*. Do *not* click the similar entries for a specific MAS under **Message Application Servers** at this time.

2. Under the voice mail domain name, double-click **Telephone User Interface**.
   a. On the **General** tab, set **Number of Digits in a Mailbox** to match the number of digits in the extension numbers on the customer PBX. If MultiSite is enabled, the Number of Digits in a Mailbox field is unavailable.
   b. Click the **Class of Service** tab.
   c. Set up classes of service (COS) for subscribers as follows.
      1. Select the **COS Number**.
      2. Update the **COS Name** to reflect this type of telephone user interface (such as *Aria TUI*, *AUDIX TUI,* or *Serenade TUI*).
      3. Select any required features for this COS and TUI.
      4. Select the appropriate **TUI type** for this COS (*Aria, AUDIX, or Serenade*).
      5. Repeat Steps 1 through 4 to set up multiple COSs. Create at least one class of service for each TUI that will be used at this site.

   Note:

   To set up a mixed environment of Aria, AUDIX, and Serenade TUIs, assign the appropriate TUI to each COS.

d. When finished, click **OK**.

e. If the system notifies you that the mailbox number changes will invalidate all previous mailboxes, click **Yes** to continue.

3. In the Voice Mail System Configuration window, double-click **Audio Encoding**.

a. In the **Audio Encoding** window, change the **Default Audio Encoding Format** to:

- **G.711 µ-Law** (mu-Law) for the United State and Japan
- **G.711 A-Law** for most other countries, especially those in Europe

Note:

The default Microsoft GSM encoding produces smaller files but poorer voice quality. Update the audio encoding to provide better sound quality, especially for IP SIP integrations. G.711 encoding is required to support TTY/TDD devices.

b. Click **OK**.

c. If you changed the audio encoding, a restart box appears. Click **OK**, but you do not have to restart now.

Note:

Although the system prompts you to restart MM Messaging Application Server service several times during this procedure, you actually must restart MM Messaging Application Server service only as directed in this guide. You must restart MM Messaging Application Server service before entering the port board extension numbers in Configuring MAS-specific parameters on page 99. You restart MM Messaging Application Server service again at the end, when configuration is complete.

Configuring the broadcast mailbox

Complete the procedure that applies to your system:

- Configuring the broadcast mailbox with a Microsoft Exchange 2010 System on page 83
- Configuring the broadcast mailbox with a Microsoft Exchange 2007 System on page 84
- Configuring the broadcast mailbox with a Microsoft Exchange 2003 System on page 85

Configuring the broadcast mailbox with a Microsoft Exchange 2010 System

Complete the following steps to assign a numeric address to the broadcast mailbox. Enter the numeric address you will use to send a message to a broadcast list.

Note:

You can perform this procedure only on an Exchange 2010 server because the Exchange 2010 Management tools cannot be loaded onto an MAS.

1. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010** > **Exchange Management Console**.

2. In the left panel, click **Recipient Configuration** > **Distribution Group**.
3. In the center panel, right-click the **BDL** group and click **Properties**.
4. In the **Properties** window, click the **E-Mail Addresses** tab.
5. **Add** a **Custom Address**.
6. In the **Custom Address** window in the **E-mail address** field, type the numeric address for the broadcast mailbox. In the **E-mail type** field, type **NUMERIC**.
7. Click **OK** to return to the **Properties** window.

Complete the following steps to restrict access to the broadcast mailbox. Enter the users with permission to send messages to the broadcast list:

1. In the **Properties** window, click the **Mail Flow Settings** tab.
2. Highlight **Message Delivery Restrictions** and click **Properties**.
3. In the **Accept messages from** field, select **Only senders in the following list**.
4. Click **Add** and select the users to add to the broadcast list. You can send messages to these users when required.
5. Click **OK** to return to the **Properties** window.

By default, the Exchange address list does not display the broadcast lists. To show the broadcast lists in the Exchange address list, complete the following optional steps:

1. In the **Properties** window, click the **Advanced** tab.
2. Clear the **Hide group from Exchange address lists** box and click **OK**.

Configuring the broadcast mailbox with a Microsoft Exchange 2007 System

Complete the following steps to assign a numeric address to the broadcast mailbox. Enter the numeric address you will use to send a message to a broadcast list.

1. Click **Start** > **All Programs** > **Microsoft Exchange Server 2007** > **Exchange Management Console**.
2. In the left panel, select **Recipient Configuration** > **Distribution Group**.
3. In the center panel, right-click the **BDL** group and select **Properties**.
4. In the **Properties** window, select the **E-Mail Addresses** tab.
5. **Add** a **Custom Address**.
6. In the **Custom Address** window in the **E-mail address** field, type the numeric address for the broadcast mailbox. In the **E-mail type** field, type **NUMERIC**.
7. Click **OK** to return to the **Properties** window.

Complete the following steps to restrict access to the broadcast mailbox. Enter the users with permission to send messages to the broadcast list:

1. In the **Properties** window, select the **Mail Flow Settings** tab.

2. Highlight **Message Delivery Restrictions** and click **Properties**.
3. In the **Accept messages from** field, select **Only senders in the following list**.
4. Click **Add** and select the users to the broadcast list. You would be able to send messages to these users when required.
5. Click **OK** to return to the **Properties** window.

By default broadcast lists are not displayed in the Exchange address list. Optionally, complete the following steps to show the broadcast lists in the Exchange address list.

1. In the **Properties** window, select the **Advanced** tab.
2. Clear the **Hide group from Exchange address lists** box and click **OK**.

Configuring the broadcast mailbox with a Microsoft Exchange 2003 System

Complete the following steps to assign a numeric address to the broadcast mailbox. Enter the numeric address you will use to send a message to a broadcast list.

Note:

You must complete this procedure on a machine where you have installed the Modular Messaging Active Directory extensions. For information about installing the Modular Messaging extensions, see Adding the Exchange extensions on page 40.

1. Click **Start** > **Programs** > **Microsoft Exchange** > **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** window, highlight the Windows domain used for Modular Messaging.
3. Select **View** and then select **Advanced Features**.
4. In the right-hand pane, double-click **Octel**.
5. In the right-hand pane, double-click the **BDL** group.
6. Select the **Modular Messaging** tab.
7. Type the numeric address for the broadcast mailbox.
8. Click **OK** to close the window.

Complete the following steps to restrict access to the broadcast mailbox. Enter the users with permission to send messages to the broadcast list:

1. In the **Properties window,** select the **Exchange General** tab.
2. In the **Message Restrictions** field, select **Only from**.
3. **Add** the users you want to be able to send messages to the broadcast list.
4. When finished adding users, click **OK** to close the window.

Configuring the PBX type

You must configure the PBX service settings for each Modular Messaging system using the appropriate configuration notes for the type of PBX or switch integration you use. Obtain the configuration notes as instructed in Downloading configuration notes on page 4. For a new installation, do this procedure on MAS#1.

Use the following steps to configure the switch integration in the **Voice Mail System Configuration** window:

1. In the **Voice Mail System Configuration** window, expand the **PBXs** item under the voice mail domain, such as *vmdom*.
2. The Modular Messaging Configuration Wizard automatically configures many settings for the certain switch integrations. Proceed as appropriate:
   - If you are using one of the automatically configured switch types, the appropriate entry is already listed under **PBXs**. Continue with Step 5.
   - If no PBX type is listed, continue with Step 3.
3. Right-click **PBXs** and select **Add New PBX Type**.
   a. For **Telephony Type**, select the type of port board that is installed in this MAS, such as *IP SIP*.
   b. In the PBXs list box, select the type of switch integration that you have, such as *Avaya SIP (IP SIP)*.
   c. Click **OK** to close this window.
4. In the **Voice Mail System Configuration** window, expand **PBXs**.
5. Double-click the PBX entry under **PBXs**.
6. Using the configuration notes for this PBX or switch, set up the specific PBX parameters required for this integration of the system.

Configuring serviceability settings

You must set up domain wide serviceability (alarming) settings once for each Modular Messaging system.

Important:
New installations of Modular Messaging support *only* SAL. For upgrades to Release 5.2, you can select SNMP, Modem Dialout or Internet alarming. For more information, see Upgrading Modular Messaging software on page 134.

Important:

If you are installing or migrating to Modular Messaging Release 5.2, SAL is the *only* remote access mechanism that Avaya supports. To activate the remote access using SAL, you must register your Modular Messaging system and the SAL gateway. For more information, see Secure Access Link 1.5 Gateway Implementation Guide. Avaya field technicians can also help you with the SAL registration.

For a new installation, perform these procedures on MAS#1.

To set up serviceability settings for the system on a new installation you must select SAL:

1. In the Voice Mail System Configuration window, double-click **Serviceability**.

   The system displays the **Serviceability - Voice Mail Domain** window.

2. 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.
3. On the **SAL destinations** tab, complete the following:
   - For **IP Address/Host**, enter the IP address or FQDN for the SAL gateway.
   - For **Community**, select a community name. This name is used as security validation in communication between the SAL client and the SAL server.
   - For **Port**, enter the port number.
4. Click **OK** to close the Serviceability - Voice Mail Domain window.
5. Proceed with Obtaining the license file on page 91.

Use the following procedure to set up the serviceability settings on a Modular Messaging system that is upgraded to Release 5.2 on which you are performing the disaster recovery.

1. In the Voice Mail System Configuration window, double-click **Serviceability**.
2. In the **Serviceability - Voice Mail Domain** window, on the **General** tab, select the type of alarming to be used for the Modular Messaging system:
   - Inactive — No alarm notification sent
   - SNMP — Send alarm traps to an NMS using SNMP
   - SAL (Default for new installations) — Use SAL to send alarms to an NMS using an agent gateway.
   - Modem dialout — Use the modem dialout to send alarm notifications to an alarm collection server for analysis and corrective actions.

   a. Internet — Relay alarm information through the internet capabilities of the Avaya SPIRIT Agent.
3. Unless directed otherwise, you can accept the default values for the following parameters:
   - The conditions for sending an alarm notification
   - The alarm level at which notification is to be sent: minor or major

- The system behavior for stopping Modular Messaging service

4. *If you selected SNMP alarming,* click the **SNMP Trap Destinations** tab. Complete the following fields:

   Note:

   For an upgrade, specify the SNMP trap destination and community details that you recorded from the R3.0, or R3.1 system in the **SNMP Trap Destinations** tab.

   - **IP Address/Host** — Enter the IP address or host name of the trap destination. Type either the IP address or the fully qualified domain name for the NMS in the field. Alternatively, click **Browse** to navigate to and select the correct NMS.
   - **Community** — Select a community name. The name is used as security validation in communication between the SNMP client and the SNMP server.
   - **Type** — Select the type of trap destination.
   - **Port** — Enter the port number.

     For additional information about completing the Serviceability General and SNMP Trap Destination information, see the VMSC — Serviceability topic in the Avaya Modular Messaging documentation.

5. *If you selected SNMP alarming,* complete the following steps to start SNMP service:
   1. Right-click **My Computer** and select **Manage**. In the **Computer Management** window, the left (Tree) pane, expand **Services and Applications**.
   2. Click **Services (Local)** in the left pane, if the item is not already selected.
   3. In the right pane, scroll down to **SNMP Trap Service**. Double-click it to open the **Properties** window.
   4. On the **General** tab, set the **Startup type** to **Automatic**.
   5. Click **Apply**.
   6. Under **Service status**, click **Start**.
   7. Wait for service to start, and then click **OK**.
   8. Minimize the **Monitor** window for later use.

6. *If you selected Internet alarming,* click the **Internet Proxies** tab. Complete the following fields:
   - **Primary Address** — Enter the Avaya proxy primary IP address or fully qualified domain name (FQDN).
   - **Secondary Address** — Enter the Avaya proxy secondary IP address or FQDN.
   - **Enable HTTP/HTPPS proxies** — Click to enable customer internet proxies.
   - **Primary HTTP/HTTPS Address** — Enter the customer proxy primary IP address or FQDN

- **Secondary HTTP/HTTPS Address** — Enter the customer proxy secondary IP address or FQDN

  For additional information about completing the Serviceability Internet Proxies information, see the VMSC — Serviceability topic in the Avaya Modular Messaging documentation.

a. If you selected *SAL alarming,* click the **SAL Destinations** tab. Complete the following fields:

- **IP Address/Host** — Enter the IP address or host name of the SAL destination. Alternatively, click **Browse** to navigate to and select the SAL destination that you want to use.
- **Community** — Select a community name. The name is used for security validation in the communication between the SAL client and the SAL server.
- **Port** — Enter the port number.

b. Click **OK** to close the **Serviceability - Voice Mail Domain** window.

Installing and configuring the WebLM server on an MAS

Modular Messaging uses WebLM as its standard licensing mechanism. Modular Messaging features are tied to the WebLM server, and any clients of that server can acquire and use a licensed feature.

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 do this, WebLM requires a license file for the product. The 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. 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.

The following three WebLM configurations are possible:

- **Existing WebLM server:** If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
- **WebLM server on an MAS or Supplementary server**:
  - For upgrades, proceed with Installing WebLM server on an MAS on page 90.
  - For new installations, the system automatically installs the WebLM server on the MAS that you select on the **WebLM Server** screen of the DCT data file.
- **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. Once you have set up and configured the WebLM server, proceed with Obtaining the license file on page 91.

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

Use this procedure to install and configure the WebLM server on an MAS or a Supplementary server.

- Installing WebLM server on an MAS on page 90
- Obtaining the license file on page 91
- Applying license file on the WebLM server on page 91
- Importing certificates from license on page 92
- Configuring the WebLM URL in VMSC on page 92

Installing WebLM server on an MAS

Complete the following steps to install the WebLM server on an MAS.

1. Log on to the MAS, on which you want to install the WebLM server as the customer account.
2. Complete one of the following steps to obtain the WebLM installer as appropriate:
   - Insert the ’Avaya Modular Messaging R5.2 MAS Application DVD 1 of 2’ disk into the DVD drive of the MAS and navigate to the ***Install\WebLM*** directory. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
   - Download the WebLM application (***WebLM_Install_Product.exe***) from the Avaya Support Web site at http://www.avaya.com/support and copy it to the MAS.
3. Double-click ***WebLM_Install_Product.exe***.

   The system runs the Web License Manager setup wizard.

   Note:

   If you are unable to install the WebLM server on the MAS, log on to the MAS using local administration credentials and continue with the installation.
4. Click **Next**.
5. Accept the default values and click **Next**.
6. In the **SSL Port** field, enter 52233.
7. Click **Next**.
8. Click **Install**.
9. Click **Finish**.

   The system displays the **WebLM Configuration** wizard.
10. Click **Next** until the configuration is complete.
11. Start the Apache Tomcat service:

a. Select **Services (Local)** in the left pane.

b. Right-click **Apache Tomcat** service.

The system opens the **Properties** window.

c. Set the **Startup type** to **Automatic**.

d. Click **OK**.

e. Click **Start** to start the service.

Obtaining the license file

Obtain a new license file from Product Licensing and Delivery System (PLDS) to be applied on a Web License Manager (WebLM) server.

CAUTION:

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

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

- If you (or 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.

To find the MAC address of the WebLM server:

1. Run the command ***ipconfig /all*** on the server where you installed the WebLM server.
2. Copy the physical address of the corporate LAN network adapter.

Applying license file on the WebLM server

Use the following steps to apply the license file on the WebLM server:

1. In the Web browser, enter the URL for the WebLM server in the format, ***https://<ip-address>:<WebLM_port>/WebLM/LicenseServer***.

   where *ip-address* is the IP address or fully qualified domain name of the server that hosts the WebLM server. For example, ***https://10.32.55.33:52233/WebLM/LicenseServer***. The URL for the WebLM is case-sensitive. The system displays the WebLM Administration page.

2. In the **Username** field, enter *admin*.

3. In the **Password** field, enter *weblmadmin*.

   Note:

   When you log on to the WebLM server for the first time after the installation, the system prompts you to change the password. You *must* change the WebLM server password to help prevent unauthorized access to the WebLM server.

4. When the system prompts you, log on to the WebLM server using the new password.
5. Click **Install License**.
6. In the **Install License Path** field, enter the path to the license file or click **Browse** to select the license file.
7. Click **Install**.

   If the installation is successful, WebLM displays a confirmation page. If you install an incorrect license file, or if WebLM cannot access the location of the license file on your network, WebLM displays an error message.

Importing certificates from license

Import the license file in VMSC to apply the certificates to your VMD.

Note:

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

1. In the Voice Mail System Configuration window, navigate to **Licensing**.
2. Right-click **Licensing** and select **Import Certificates from License**.

   The system opens the **License Import Wizard**.
3. Complete the wizard.
4. Restart the Messaging Application Server service on all MASs.

Configuring the WebLM URL in VMSC

Configure the URL for the WebLM server in VMSC on the MAS:

1. In the Voice Mail System Configuration window, double-click **Licensing**.

   The system displays the **Licensing - Voice Mail Domain** window.

2. 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://10.32.55.33:52233/WebLM/LicenseServer.***

   b. Click **OK**.

3. Restart the Apache Tomcat service for the changes to take effect.

4. Restart the Messaging Application Server service on all MASs as outlined in Restarting messaging services on page 102.
5. On the **Licensing** tab, in the **License Mode** field, verify that the system displays the status as **Normal**.

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

Entering Product ID for current MAS

If Avaya is to support this system, you must enter the MAS product ID that ART (Automatic Registration Tool) provides. You can view the product IDs using Maestro.

1. From the VMSC (**Start** > **Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration**), double-click **Message Application Servers**.
2. Double-click the MAS you are currently configuring and select **Serviceability**.
3. On the **Serviceability** window, type the product ID for the MAS in the **Product Identifier** field.
4. Click **OK**.

Configuring specific features as needed

During installation, MMCW enables services and TTS languages specified in the DCT data file. However, 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 TTS, if necessary. Unless otherwise specified, you can configure these features on any MAS in the VMD.

Note:

The following are important notes about configuring these features:

- You must have the relevant permissions to configure screens in the VMSC application. For more information about security roles required for VMSC configuration, see *Avaya Modular Messaging MAS Administration Guide*.
- If any of these features is enabled improperly or on the wrong server by the MMCW, manually configure the affected feature. For more information on moving the services to another server, see Moving Modular Messaging services among servers on page 257.
- If you are enabling the MultiSite feature, see *Avaya Modular Messaging MultiSite Feature Description Guide* to configure the MultiSite specific features. For information on MultiSite specific configuration, see the **Voice Mail System Configuration** section in *Avaya Modular Messaging MAS Administration Guide*.

To configure specific features for the VMD:

1. Use the Voice Mail System Configuration program.

   If this window is not already open, click **Start** > **Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration**.

2. After all MASs in the system have been installed, configure the features that are required for the VMD.

   - Configuring Call Me service on page 94
   - Configuring Notify Me on page 94
   - Configuring MWI service on page 95
   - Configuring languages and multi-lingual TTS on page 95
   - Configuring Audit Service on page 96
   - Configuring the MM Fax Sender server on page 96
   - Configuring offline access to messages on page 98

Configuring Call Me service

Complete the following steps to configure Call Me Service for the VMD:

1. Under the voice mail domain, double-click **Call Me**.
2. On the **General** tab, click the checkbox to **Enable Call Me**.
3. For **MAS Call Me server**, enter the name of the MAS or supplementary server on which the MM Call Me Server service is installed. You can use the browse button (...) to locate the server.
4. Click **OK**.

Note:

Because the Call Me server and Message Waiting Indicator (MWI) Server both use the Mailbox Monitor Server, they must be installed on the same server.

Configuring Notify Me

Complete the following steps to configure Notify Me for the VMD:

1. Under the voice mail domain, double-click **Notify Me**.
2. On the **General** tab, click the **Enable Notify Me** checkbox.
3. Click **OK**.

Configuring MWI service

Complete the following steps to configure MWI service for the VMD:

1. Under the voice mail domain, double-click **Message Waiting Indicator**.
2. On the **General** tab, click the checkbox to **Enable Message Waiting Indicator (MWI)**.
3. For **MAS MWI server**, enter the name of the MAS or supplementary server on which the MM Message Waiting Indicator Server service will be running. You can use the browse button (...) to locate the server.
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** box, list all MASs that have a port group set up to support MWI. To add a server name:
   a. Double-click inside the top of the big list box, or click the **Add** button just above 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 each MAS that has ports allocated to support MWI.
   d. Repeat Steps b and c to add any other MASs that support MWI, such as *MYMAS2*.
   e. Click **OK** to close this window.

      The arrow icons move the selected MAS up or down the list. MWI requests start with the first MAS in the list, and continue to each additional MAS if needed.
6. Click **OK** to close the **Message Waiting Indicator - Voice Mail Domain** window.

Configuring languages and multi-lingual TTS

To configure multiple languages or the optional Text-to-Speech (TTS) feature:

Note:
Enable Multi-Lingual TTS only if it is required at the site.

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 the Multi-Lingual Text-to-Speech (TTS) feature is required at this site:*
      1. Click the **Enable Multilingual Text-to-Speech** check box.
      2. In the list box, select all the languages to use for TTS at this site.
3. Click **OK** to close this window.

Configuring Audit Service

Complete the following steps to configure MAS auditing for the VMD.

1. In the **Voice Mail System Configuration** window, under the VMD, double-click **Auditing**.
2. On the **General** tab, click the check box to **Enable Auditing**.
3. In the **Audit server** field, enter the name of the server that will run the MM Audit service, or use the browse button (...) to select the name.

   MM Audit service is installed and running on each MAS and supplementary servers in the VMD. The name that you enter here is the name of the MAS or supplementary server that acts as the MM Audit Server.
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 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. For more information, see *Avaya Modular Messaging MAS Administration Guide*.

Configuring the MM Fax Sender server

These steps describe how to configure Avaya's native fax support. When configuring third-party fax support, see the appropriate Fax Configuration Note on the Avaya support website. For additional information, see *Avaya Modular Messaging MAS Administration Guide*.

Complete these steps on the MAS in your VMD that is running the Modular Messaging Fax Sender server.

Note:

To configure the **Fax** dialog box in **VMSC**, you must be a member of a security role that is assigned the Fax-Administer task.

To configure MM Fax Sender server:

- Configure the MM Fax sender server in VMSC
- Share the Microsoft Fax Printer
- Assign permissions to the Fax Service Manager
- Create a dialing rule

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

1. In the **Voice Mail System Configuration** window, under the VMD, double-click **Fax**.
2. On the **General** tab:
   a. Click the check box for **Fax Enable**.
   b. Click the check box to **Use native fax support**.
   c. For **MAS Fax Sender server**, enter the name of the MAS where MM Fax Sender Server service is installed, or **Browse** to locate the server.
   d. **Fax Mailbox** displays the name of the fax mailbox, which is used for outgoing faxes on the Exchange message store server. This field is populated automatically and cannot be edited.
   e. For **Company Fax Number** enter the externally dialable number that callers must use to send faxes to subscribers. This number appears on outgoing fax cover pages.
3. Click the **Advanced** button.
   a. In the Advanced Fax window, change the **Max Concurrent Outgoing Calls** number to the customer-specified number.
   b. Adjust other options if required.
   c. Click **OK** to close this window.
4. Click **OK** to close the **Fax - Voice Mail Domain** window.

   The system displays a "restart" window.
5. Click **OK**.

Complete the following steps to share the Microsoft Fax Printer:

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 **Sharing** tab.
5. Select the **Share this printer** check box. Leave the share name as **Fax**.
6. If not already added, add **Everyone** to the list of users and groups with access.
7. Assign **Fax** permission to **Everyone**.

Complete the following steps to assign permissions to the Fax Service Manager:

1. Select 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. Make sure that **Everyone** is assigned **Fax** permissions for the Fax Service Manager.
8. Exit all windows.

Note:

If the System Administrator wants to restrict access to the Fax printer at a later date, complete the following changes to the Fax printer share and Fax Service Manager:

1. Remove **Everyone** from the list of users and groups with access.
2. Add Active Directory users and groups that need to print faxes using the MM Fax Printer to the list of users and groups with access.
3. Assign **Fax** permission to the Active Directory users and groups.

Complete the following steps to create a dialing rule for the Phone and Modem:

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

Configuring offline access to messages

CAUTION:

Set up offline access only after all servers in the system are configured, including the supplementary server, if present. Before you can configure offline access, you must create the offline message store. For more information, see the *Avaya Modular Messaging MAS Administration Guide*.

To configure offline access to subscriber messages:

1. In the **Voice Mail System Configuration** window, under VMD, such as *vmdom*, 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. If this system has multiple MASs:
   a. Select the **Synchronize offline messages with remote store** check box.

b. Click **Browse** to select an existing, shared directory in the domain for the remote offline message store. If the directory does not exist, create it first, then browse to the directory.

The name must use the format ***locationname**sharename***, such as *mymas2**RemoteOfflineStore*.

5. Change other parameters in this window as needed. For more information, see the *Avaya Modular Messaging MAS Administration Guide*.
6. Click **OK** to close this window.

Configuring MAS-specific parameters

After you configure the domain-wide parameters, complete the configuration of this specific MAS in the VMSC. Do the procedures in this section under the specific entry for this MAS, and not under the voice mail domain.

Complete the tasks in this section on each MAS as required:

- Configuring INADS alarming, if used on page 99
- Configuring port boards and switch integration on page 100

When you configure some MAS-specific parameters, you will need to select the MAS in the Voice Mail System Configuration window. If the MAS you are configuring does not appear in this window, refresh the window.

Configuring INADS alarming, if used

If this MAS uses INADS alarming, configure the service now. You must administer INADS alarming individually for each server and supplementary server that uses INADS alarming. The server requires a modem and the Messaging Application Server service to be installed for INADS alarming to work.

To set up INADS alarming on this MAS:

1. In the **Voice Mail System Configuration** window, expand **Message Application Servers**.
2. Expand the entry for this MAS, such as *MYMAS1*.
3. Double-click **Serviceability**.
4. Click the **INADS** tab.
5. Complete the following fields:
   a. **COM port** — Select the communications port that the modem is to use to make calls for alarm notification. Avaya recommends COM3 for the recommended USB port on the MAS.

b. **Phone number** — Enter the complete telephone number the modem must dial to place an alarm notification with the remote service center. Include any special characters needed. For example, to access an outside line, insert pauses, and so on.

c. **Modem setup** — Enter the modem initialization (setup) string required for the modem to make alarm notification calls.

For additional information about completing the MAS - Serviceability - General and MAS - Serviceability - INADS information, see the VMSC — Serviceability topic in the Avaya Modular Messaging documentation.

6. Click **OK** to close this window.
7. If prompted, restart the MAS service.

Configuring port boards and switch integration

Note:

You must restart service at the end of the previous procedure before continuing.

The Modular Messaging Configuration Wizard automatically configures many of the port board and PBX settings for the MAS. However, you must always verify the configuration settings against the most current configuration notes.

Note:

The configuration notes for this PBX or switch might include some of these steps. However, read through this section first to get an overview of the configuration procedure. You can repeat steps to verify the setup. You can also update or change this information later if required.

Automatic configuration

The Modular Messaging Configuration Wizard automatically configures the MAS settings for the following switch integrations:

- Avaya SIP
- Avaya (IP H323)
- Avaya (QSIG)
- Cisco (QSIG)
- Nortel NT M-1 (QSIG)
- Siemens Hipath (QSIG)

If you are using one of these switch types:

1. Verify the MAS settings against the configuration notes in case of changes.
2. Administer all required settings on the switch.

Manual configuration

If you specified **Other** for the switch integration type, you must always configure both the MAS settings and the switch settings for each MAS.

To set up the basic PBX integration details for each MAS in this domain:

1. In the **Voice Mail System Configuration** window, expand **Message Application Servers**.
2. Expand the entry for this MAS, such as *MYMAS1*.
3. Right-click the server name, and then select **Telephony Configuration Wizard**.
4. Complete all steps in the wizard, as prompted. Use the configuration notes as required.
5. After you complete the wizard, restart messaging service so that you can configure the voice ports:
   a. Restore the **Monitor** window if you minimized it, or access the window to monitor services using one of these methods:
      - Double-click the **Monitor** icon on the desktop (if present). In the left pane, click **Services** if it is not already selected.
      - Right-click **My Computer** and select **Manage**. In the left (Tree) pane, expand **Services and Applications**, and then click **Services**.
   b. Click **Service (Local)** in the left pane, if the item is not already selected.
   c. In the right pane, scroll down to **MM Messaging Application Server**. Right-click it and select **Stop**.
   d. When service is stopped, right-click **MM Messaging Application Server** again and select **Start**.

      The system restarts the MM Messaging Application Server service.

   Note:

   When you restart messaging service, the Monitor window immediately shows a status of **Started**. However, the service might actually take several minutes to start, depending on the number of port boards installed and the integration method.

   e. Track the startup progress as follows:
      1. Access the event viewer using one of these methods:
         - In the **Monitor** window, in the left pane, expand **Event Viewer (Local)**.
         - In the **Computer Management** window, in the left pane, expand **System Tools**, and then **Event Viewer**.
      2. In the left (Tree) pane, click **Application**.
      3. Refresh the window display periodically until you see Telephony User Interface event 1241, **TUI service has been enabled**. You can then proceed.
   f. When service is restarted, minimize this window.

6. In the **Voice Mail System Configuration** window, expand **Message Application Servers**.

   Note:

   Some values might already be set. Follow the configuration notes for this PBX integration.

   a. Expand the entry for the MAS (such as *MYMAS1*).

   b. Double-click **Telephony Interface**. Configure the port boards in this MAS. Use the configuration notes; see Downloading configuration notes on page 4

   c. Double-click **PBX Type**. Select the same type of PBX service as you did in Configuring the PBX type on page 86. Verify that the entry in the **PBXs** box is highlighted, and click **OK**.

   d. *If multiple port groups are used,* double-click **Port Groups**. For example, you might use a unique group to support MWI.

   e. Double-click **PBX Integration** and configure the integration type for this system. Use the configuration notes to specify or confirm the settings this switch integration requires.

Restarting messaging services

When you complete configuring the server, restart the messaging services:

1. Restore the **Monitor** window if you minimized it, or access the window to monitor MM Messaging Application Server service using one of these methods:
   - Double-click the **Monitor** icon on the desktop (if present). In the left pane, click **Services** if it is not already selected.
   - Right-click **My Computer** and select **Manage**. In the **Computer Management** window, the left (Tree) pane, expand **Services and Applications**, and then click **Services**.
2. In the left pane, click **Service (Local)**.
3. Restart MM Messaging Application Server service to accept any changes you made in the VMSC:

   a. In the right pane of the **Monitor** window, scroll down to **MM Messaging Application Server**. Right-click it and select **Stop**.

   b. When service is stopped, right-click **MM Messaging Application Server** again and select **Start**.

   The system restarts the messaging service.

   When you restart MM Messaging Application Server service, the **Monitor** window immediately shows a status of **Started**. However, service might actually take several minutes to start, depending on the number of port boards installed and the integration method.

c. Track the startup progress as follows:

1. Access the event viewer using one of these methods:
   - In the **Monitor** window, in the left pane, expand **Event Viewer (Local)**.
   - In the **Computer Management** window, in the left pane, expand **System Tools**, and then **Event Viewer**.
2. In the left (Tree) pane, click **Application**.
3. 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 all messaging services required for this MAS are started:

a. In the **Monitor** window, click **Services (Local)** in the left pane, if the item is not already selected.

b. In the right pane, scroll down to the list of Modular Messaging services. All services start with the abbreviation **MM**. Verify that the **Status** column shows the correct state for each messaging service:

- Services that are required for this server must show **Started** and a startup type of **Automatic**.
- Services that are not required on this server must show a blank status and a startup type of **Disabled**.

Complete the following steps if necessary to change the status.

c. If the **Startup Type** for any **MM** service that is *not* required for this server is **Manual**:

1. Double-click the service to open the **Properties** window.
2. Set the **Startup type** to **Disabled**.
3. Click **OK** to close this window.
4. Refresh the screen to verify that all **MM** services *not* required for this server are **Disabled**. Repeat Step c as needed.

CAUTION:

All **MM** services that are *not* required for this server must be set to **Disabled**. Serious problems occur if you activate a service that is supposed to run on only one server in the VMD on multiple servers.

5. *For a multiple-MAS system,* after you configure the last MAS and install the license file, restart MM Messaging Application Server service on all servers in the VMD. A restart ensures that the voice mail domain-wide properties are consistent across the VMD. To restart service on all MASs in the voice mail domain:

a. Switch the monitor to show the next MAS in the system.

b. Repeat Steps 3 and 4 to restart service.

c. Repeat this procedure for each MAS in the system.

Verifying basic operation of this MAS

Complete the following tests to verify the basic functionality of this MAS.

- Verifying call-handling capability on page 104
- Verifying alarming setup on page 104
- Verifying Tracing Service operation on page 105
- Verifying Audit Service on page 106

Verifying call-handling capability

Perform this task on each MAS that is set up to handle calls.

This test confirms basic connectivity between the MAS and the switch.

1. If this MAS is in a multiple-MAS system, display the port monitor to ensure that the test call comes in on this MAS. For this procedure, see Setting up the port monitor on page 111.
2. From a telephone on the system, dial the message retrieval number for the Modular Messaging system.
3. Listen for the Modular Messaging system to answer.
4. Hang up.

Verifying alarming setup

Perform this task on any MAS that is set up for INADS, SNMP, or SAL alarming. This test does not work if alarming is set to **None**. To confirm the serviceability settings used at this site, see Configuring serviceability settings on page 86.

This test requires the receiving computer, either INADS, SNMP or SAL, to be set up by the appropriate party and ready to receive alarms.

To verify that alarm notification is working:

1. Click **Start** > **Run**.
2. In the **Run** window **Open** field, type **cmd** and press **Enter**.
3. In the command prompt window, type the following and press **Enter**:

   testaom -v

   The test shows the type of alarming that is set up (INADS, SNMP or SAL), the product ID for the MAS, and the alarming settings. The test takes about 1 minute to run.

4. Verify that the last line of the test reads:

   Alarm origination test successful

   Continue with Step 6.

5. *If the alarm test fails,* the last line of the test reads:

   Negative acknowledgement of transmission

   If the test fails, check your alarming settings, and then run the test again:

   - *For all systems,* see Configuring serviceability settings on page 86.
   - *For the systems that use INADS,* also check Configuring INADS alarming, if used on page 99.

6. Type **exit** and press **Enter** to close this window.

   Note:

   For instructions on accessing the MAS alarm or error logs, see the *Avaya Modular Messaging MAS Administration Guide*.

Verifying Tracing Service operation

If you enabled the Tracing Server software on an MAS or a supplementary Tracing server, test the Tracing System operation as follows:

1. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Operational History Viewer**.
2. Set up a live mode session for all MASs in the voice mail domain (VMD):
   a. In the **Operation History Viewer** window, click **File** > **New**.
   b. In the **Session Properties** window, verify that **Message Application Server** shows **All Servers** is selected.
   c. Click the check box for **Live Mode**.
   d. Verify that all the **Select Types** check boxes are checked.
   e. Under **Selection Activities**, verify that the **All Activities** check box is checked.
   f. Click **OK** to close this window.
3. Confirm that the Tracing Server can connect to all MASs in the VMD.
4. Confirm that the Operation History Viewer (OHV) displays the collected operation history events.
5. You can close the OHV, or keep it open to monitor acceptance tests. For more information, see Using the Operational History Viewer on page 110.
6. If you close the OHV, the system might prompt you to save the session. Click **No**.

Note:

For more information about using the Operation History Viewer, see the *Avaya Modular Messaging MAS Administration Guide*.

Verifying Audit Service

Use the MM Audit Log Viewer to view information captured by the MM Audit Service:

1. Click Start > Programs > Avaya Modular Messaging > MM Audit Log Viewer.
2. To connect to the database on the Audit server (complete these steps only if you are running the viewer on an MAS that is not the Audit server):
   a. On the **MM Audit Log Viewer** window, in the left-hand pane, right-click **All Events**.
   b. Click **Connect to Database**.
   c. In the **Server** field, enter the name of the MAS you set up as the Audit server.
   d. Click **Connect**.
3. On the **MM Audit Log Viewer** window, in the left-hand pane, click **All Events**.
4. In the right-hand pane, verify that events appear in the Audit Log.
5. Close the **MM Audit Log Viewer** window.

For more information, see *Avaya Modular Messaging MAS Administration Guide*.

Continuing the installation

If you have additional MASs to configure, return to Configuring an Avaya MAS on page 45 or Configuring a customer-provided MAS on page 59.

If you have configured all MASs, continue to Testing and backing up the system on page 107.

Chapter 7: Testing and backing up the system

This chapter describes how to perform acceptance tests to verify that the Modular Messaging system is providing full service. After functionality is verified, back up the system to protect the Modular Messaging configuration data.

Note:

Before you can successfully complete the tasks described in this section, you must have successfully completed the tasks in Chapter 6: Configuring the voice mail system on page 79.

Topics in this chapter include:

- Adding a test subscriber on page 108
- Setting up monitoring tools—optional on page 110
- Performing acceptance tests on page 112
- Removing the test subscribers on page 118
- Backing up the system on page 119
- Turning over the system to the customer on page 120

Adding a test subscriber

For a new installation, the directory server administrator previously created test subscriber accounts for each telephone user interface. See Creating test subscriber accounts on page 14. Before you can complete the acceptance tests, the administrator must assign Modular Messaging characteristics to these accounts.

Note:

If you are performing tests following a Modular Messaging software upgrade, you might want to test the system using subscribers that are already administered.

For details on administering Modular Messaging features, see Chapter 15, “Creating subscriber accounts for Microsoft Exchange," in the *Avaya Modular Messaging MAS Administration Guide*.

Complete the following sets to set up the test subscribers.

1. Log on to the Active Directory server using an account that has privileges to create new user accounts (such as *administrator*).

   Note:

   The Modular Messaging Active Directory Extensions must have been installed on the server before you can administer any subscribers. For additional information about the Modular Messaging Extensions, see Adding the Exchange extensions on page 40.

2. Click **Start** > **Programs** > **Microsoft Exchange** > **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** window, expand the directory for the Windows domain you used for Modular Messaging.
4. In the left pane, click **Users**.
5. In the right pane, double-click a test subscriber account, such as *Aria Test Subscriber (testsub1),* to open the **Properties** window.
6. Click the **Modular Messaging** tab.

   Note:

   The first time you access this tab, you might see a **Choose Message Application Server** window. Enter the name of an MAS (or click **Browse** to select it), and then click **OK**.

   There might be a delay as the server logs in.

7. Set up the test subscriber with Modular Messaging features as follows:
   a. Click the check box to **Enable Modular Messaging**.
   b. Verify the voice mail domain (VMD).
   c. Enter the extension number, mailbox number, numeric address, and TUI password.

Note:

The numeric address must be unique among all the addresses in the messaging network. For example, you could prepend a **1** or the area code to the mailbox number.

All extensions for the test subscribers must be administered on the PBX by the appropriate party.

d. Click **Advanced**. In the **Advanced Properties** window:

1. Select the appropriate **Class of service** for this test subscriber (for example, *Aria TUI*, *AUDIX TUI, or Serenade TUI*).
2. In the **Capabilities** field, under **Message assistant**, click the check box to **Allow Message Waiting Indicator**.
3. Click the appropriate check boxes to activate any other features that you have installed and must test at this site.
4. Click **OK** to close this window.

e. When finished setting up this test subscriber, click **OK**.

8. To set up another test subscriber (for example, to test the MM AUDIX or MM Serenade telephone user interface), repeat Steps 5 through 7.
9. Although Message Waiting Indicator has been allowed, it must also be enabled for each test subscriber.
   a. Right-click **My Computer** and select **Manage**.
   b. In the **Computer Management** window, in the left pane, expand **Event Viewer**.
   c. Refresh the window display periodically until you see a **1027** event. You must see the 1027 event before you can proceed.
   d. In the **Active Directory Users and Computers** window, double-click the first test subscribers.
   e. Select the **Modular Messaging** tab.
   f. On the Modular Messaging tab, click **User Options**.
   g. In the **Assistant** window, click the **Message Waiting Indicator** box and the box for any other capabilities that you have previous activated and that you intend to test.
   h. Click **OK** to close this window.
   i. Repeat steps d through h for each test subscriber.
10. When finished, click **OK** to close the **Active Directory Users and Computers** window.

Setting up monitoring tools—optional

You can use the monitoring aids described in this section to help you complete the acceptance tests.

Using the Operational History Viewer

You can use the Operational History Viewer (OHV) to monitor call progress for any MAS. The viewer can help to identify the cause of the problem if errors occurs during testing.

Note:

If you are running the OHV on an MAS that is not running the tracing server service, you must first configure your data sources. For additional information, see the discussion about selecting a data source and ODBC tracing in the *Avaya Modular Messaging MAS Administration Guide*.

To open the Operational History Viewer:

1. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Operational History Viewer**.
2. Set up a live mode session for all MASs in the voice mail domain (VMD):
   a. In the history viewer window, click **File** > **New**.
   b. In the **Session Properties** window, verify that **Message Application Server** shows **All Servers** is selected.
   c. Click the check box for **Live Mode**.
   d. Verify that all the **Select Types** check boxes are checked.
   e. Under **Selection Activities**, verify that the **All Activities** check box is checked.
   f. Click **OK** to close this window.
3. During testing, monitor Operation History events in the Viewer. The OHV displays events as they happen on the system.
4. After testing is complete, close the OHV.
5. If the system prompts you to save the session, click **No**.

Setting up the port monitor

This task is optional for a one-MAS system, but is recommended for a system that has multiple MASs that are set up to take calls.

Tests calls can come in through the ports on various MASs in the system, depending on how the hunt group is set up on the PBX. If the Modular Messaging system has more than one MAS, use the port monitor to verify that the test calls you make are coming in on the ports of the MAS that you want to test.

To display the port monitor:

1. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Port Monitor**.
2. When the system prompts for the Message Application Server, select the MAS that you want to test (such as *MYMAS1*). Click **Select**.

   The **Port Monitor** window for this MAS is displayed.
3. You can repeat Steps 1 and 2 to bring up **Port Monitor** windows for multiple MASs if desired.
4. When you dial the Modular Messaging system message retrieval number during the acceptance tests, check the **Port Monitor** window to verify that the call is coming in on a port of the MAS that you want to test.
5. If the port monitor does *not* show that the test call is coming in on the desired MAS, hang up and dial the Modular Messaging system message retrieval number again.

   The number of times you might have to dial depends on the switch administration. For example, the hunt group might be administered to send each new call to the next MAS in the system, or it might be administered to send all the calls to one MAS before it moves on to a subsequent MAS.

Performing acceptance tests

Complete the following tests on each MAS that is set up to handle calls.

CAUTION:

Wait 5 minutes after completing the tasks in Chapter 6: Configuring the voice mail system on page 79 to give the system time to update all servers in the voice mail and Windows domains with the correct Modular Messaging information.

Creating and sending a call-answer message

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

To create and send a call-answer test message:

1. Call the MM Aria test-subscriber extension from any other telephone. Allow the Modular Messaging system to answer.
2. Speak into the telephone and record the following or a similar test message after the tone:

   "This is a test call answer message."
3. Hang up the telephone to disconnect.
4. Repeat Steps 1 through 3 for each TUI that you are testing.

Retrieving test messages in integrated mode

Test the fully integrated operation of the system as directed. You need access to the actual telephone whose extension number is assigned to the test-subscriber mailbox to perform this test.

To verify the receipt of the test messages in integrated mode:

1. *If MWI is installed:* 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 phone.

   Note:

   The message-waiting lamp might 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 call was received:

   a. Verify that the Mailbox Monitor and MWI services are started.

1. Access the window to monitor services using one of these methods:
   - Double-click the **Monitor** icon on the desktop (if present). In the left pane, click **Services** if it is not already selected.
   - Right-click **My Computer** and select **Manage**. In the **Computer Management** window, the left (Tree) pane, expand **Services and Applications**, and then click **Services**.
2. In the right pane, scroll down to the Modular Messaging (MM) services. Verify that the Status column shows that service is **Started** for each installed messaging service.
3. If service is stopped or if the Status column is blank, right-click the appropriate MM service and select **Start**.
4. When finished, click **OK** to close this window.

b. If service is started, check for a problem with the test subscriber administration, the switch integration or switch integration software, or the switch number administration for the test telephone.

2. From the test-subscriber telephone, dial the Modular Messaging system message retrieval number.
3. Enter the password for this mailbox and press #.

   The system voices the name of the test subscriber.
4. 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.
5. After the mailbox is set up, retrieve the test message.

   The system uses different commands to retrieve messages depending on whether you are using the Aria or AUDIX user interface.

To retrieve a test message using the MM Aria interface:

1. After the mailbox is set up:
   a. Press **1** to review the new messages.
   b. Press **1** to retrieve a voice message.
   c. Listen to the message. If the message does not play properly, contact the remote support center.
   d. Press **7** to erase this message.
   e. Repeat Steps c and d to review the next message (if any), or press ***** to return to the main menu.
2. Hang up the telephone to disconnect when finished.
3. 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.

To retrieve a test message using the MM AUDIX interface:

1. After the mailbox is set up:
   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 *** D** (or *** 3**) to erase this message.
   d. Repeat Steps b and c to review the next message (if any), or press *** R** (or *** 7**) to return to the main menu.
2. Hang up the telephone to disconnect when finished.
3. *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.

To retrieve a test message using the MM Serenade interface:

1. After the mailbox is set up:
   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.

Creating and sending a test message in nonintegrated mode

The system uses slightly different commands, depending on the telephone user interface you have. Differences are noted in the text.

To create and send a test message in nonintegrated mode:

1. Dial the Modular Messaging system message retrieval number from any telephone that is not administered on the system.

   The system voices the "Welcome to Avaya Messaging" prompt.
2. Press **#** to skip the system introduction.
3. Enter the extension number for test-subscriber mailbox.
4. Enter the password for this mailbox and press **#**.

   The system voices the name of the test subscriber.
5. To create a new 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 **#** to approve the message.
8. When the system prompts you, enter the mailbox number for any other test subscriber when prompted for the extension. Then press **#**.

   The system voices the name of the test subscriber.
9. To approve the message and address list:
   - On the MM Aria interface, press **#** twice (as prompted).
   - On the MM AUDIX interface, press **#**.
   - On the MM Serenade interface, press the pound key (**#**) twice.
10. Press **#** 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 on page 112.

Testing the outcalling capability

Test the outcalling capability of the system using the Modular Messaging (MM) Client software, also known as the Avaya Modular Messaging Subscriber Options package.

To test system outcalling:

1. Run this test from any machine where the Subscriber Administration extensions are installed. For details, see Adding the Exchange extensions on page 40.
2. Click **Start** > **Programs** > **Microsoft Exchange** > **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** window, expand the directory for the Windows domain you used for Modular Messaging.
4. In the left pane, click **Users**.
5. In the right pane, double-click a test subscriber account and open the **Properties** window. For complete steps, see Steps 3 through 5 in Adding a test subscriber on page 108.
6. Click the **Modular Messaging** tab.
7. Click **User Options** to run the Modular Messaging client software.
8. Click the **Media Setup** tab.

9. Set up the recording and playback options to use a telephone near you:
   a. For **When composing voice messages**, select **Telephone**.
   b. Click **Configure**.
   c. In the **Telephone Properties** window, enter the extension number of a telephone near you.
   d. Select or enter the name of this MAS if needed. Click **OK**.
   e. For **When reviewing voice messages**, select **Telephone**.
   f. Repeat Steps b through d to set up telephone playback.
10. Re-record the recorded name. For example:
    a. *On an Exchange 2003 system:* In the **Modular Messaging User Properties** window, click the **Record Greetings** tab.
    b. Verify that the telephone will be used for recording and playback:
       1. Check the icon to the left of the status display. If it shows a telephone, continue with Step c.
       2. If the icon shows a terminal, right-click and select **Telephone**. The icon changes to show a telephone. Continue with Step c.
    c. Under Standard Greetings, select **Spoken Name**.
       1. Click **Record** (the red circle) on the player near the bottom of the window.
       2. When the telephone rings, answer it and record a name for the test subscriber after the tone.
       3. When finished, click **Stop** (the black square) on the player.
       4. Click **OK**.
11. Play back the spoken name to test outcalling, as follows:
    a. Click the **Play** button (large black single arrow) on the player near the bottom of the window.
    b. Answer the telephone when it rings.

       The picture of the phone changes to become off-hook.
    c. Listen for the system to play the spoken name of the test subscriber.
    d. Hang up the telephone.

       The picture of the phone changes back to being on-hook (this might take a couple of seconds).
    e. Click **OK** to close the **Modular Messaging User Properties** window.
12. When finished, close all open windows.

Creating and printing a fax message

Do this test only under the following circumstances:

- The MM Fax Sender server is installed in the VMD
- Perform this test on the MAS hosting the fax printer

To create and send a test fax message:

1. From a fax machine, send a fax to the test subscriber mailbox. This subscriber mailbox must be set up to be fax enabled.
2. Wait a few minutes for the fax to be delivered. The MWI lamp, if present, on the test subscriber telephone should light.
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 voices the name of the test subscriber.
7. Retrieve and print the fax as follows:
   - On the MM Aria interface:
     a. Press **1** to retrieve new messages.
     b. Press **3** to retrieve the fax message.
     c. After the prompt finishes, press **2** and follow the prompts.
   - On the MM AUDIX interface:
     a. Press **2** to retrieve new messages.
     b. Press star (*****) **1** to print the fax.
     c. Press star star (******) **6** and follow the prompts.
   - On the MM Serenade interface:
     a. Press **1 9** to retrieve new messages.
     b. Press **8** to print the fax.
     c. Press **3** and follow the prompts.
8. Verify that the fax prints correctly.
9. *If MWI is installed,* check the MWI on the test subscriber telephone again. The MWI should be off.

Running additional tests

You might want to run additional tests to verify the correct operation of features that are particularly important to the customer. For example:

- Automated Attendant
- Call Me
- Find Me
- Octel Analog Networking

To test these or other features, see the *Avaya Modular Messaging MAS Administration Guide* for feature setup and operation instructions.

Removing the test subscribers

When acceptance testing is complete, remove any test subscribers using the normal procedures for this version of Microsoft Exchange. For example:

1. Log in to the directory server using an account that has privileges to delete user accounts (such as *administrator*).
2. Access Active Directory Users and Computers.
3. Expand the directory for the Windows domain you used for Modular Messaging.
4. In the left pane, click **Users** or **Recipients** as required.
5. In the right pane, right-click each test subscriber and select **Delete**.

Backing up the system

Before you back up the system, perform a complete DCT analysis of the supplementary server and all MASs. For more information, see Using the DCT to collect information from an MAS on page 130 or see the DCT online help system or its printed version, *Avaya Modular Messaging Data Collection Tool Help*, for a complete description of the procedure to analyze a system.

As a final installation task, set up the system to perform regular, scheduled backups of MAS-specific information using the normal backup procedures for this site. Avaya recommends that you do an attended backup now on each MAS to preserve the configuration information and to verify the backup function.

Customers should consider the following when designing their backup program:

- *DCT data file*: Be sure to include the most recent DCT data file in your regular backups. Periodically analyze your system with the DCT executable file (**MMDCT.exe**) to create a new updated data file to use in case of a disk failure. This is particularly important when changes are made to the Modular Messaging system. See the DCT online help system or its printed version, *Avaya Modular Messaging Data Collection Tool Help*, for a complete description of the procedure to analyze a system.
- *Customized tone files*: Avaya suggests that all tone files be stored in the \Avaya_Support\Tone_Files directory. You might choose to back up this location or store a copy of the tone files elsewhere for backup.
- *Customized prompt files:* Keep a copy of customized prompt files stored in the **CustomPrompts.ovf** and **CustomPrompts_G711.ovf** files. The files are stored in the path c:\program files\avaya modular messaging\vserver.
- *Caller applications:* Caller Applications (*.uma files), once deployed, are stored on each MAS within a folder that has a GUID. The location for this folder is **\Program Files\Avaya Modular Messaging\VServer\CallerApps**. Avaya recommends that you back up a copy of this folder as follows:

  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).
- *Licensing files:* Keep a backup of the licensing files (*.xml) safe on another device or in another location.
- *SIP certificates :* For SIP implementations only, backup certificates and related files. From \Program Files\Avaya Modular Messaging\OpenSSL, backup the following files:
  - **AVA\dh1024.pem**, **certchain.crt**, and **certchain.key**
  - **CommonTrust\AvayaRoot\avayaprca.crt** and **sip_product_root.crt**.
  - **CommonTrust\CaHash\465bb314.0** and **ffbc7d70.0**

- *WSO:* Backup **Program Files\Avaya Modular Messaging\Web Subscriber Options\ masinfo.cfg**.
- *VMD account and Exchange mailbox*: Back up the VMD account and Exchange users mailbox.
- *Audit Database*: Follow Microsoft recommended SQL Server procedures to backup the MM Audit Database.
- *Operation History* and *Transaction Databases*: Used by the MM Tracing Server and MM Reporting Tool. From \Program Files\Avaya Modular Messaging\Tracing, backup the following files:
  - trxdb.mdb
  - ophist.mdb

  Schedule the backup of these files before nightly cleanup processes are scheduled to run.

Running periodic checks

Perform scheduled maintenance on the MAS routinely to keep the hard disk in good condition. Run the following on a regular basis:

- Disk Defragmenter system tool
- **chkdsk** command

Turning over the system to the customer

At this point, the system is considered ready for handoff to the customer. Handoff considerations include:

1. Hand over the latest analyzed DCT data file to the customer. Then erase the file from your USB storage device.
2. Advise the customer about the initial administration that was completed. The customer might want to customize features such as:
   a. Any feature parameters in the Voice Mail System Configuration (VMSC) program.
   b. The classes of service to use for subscribers might need to be updated or expanded.
3. Advise the customer about the ongoing administration that is required, such as customizing parameters, installing client packages, and maintaining the system. For more information, direct the customer to the administration topics in the documentation library.

The system is set up to send alarming information and receive incoming technical support calls. Customers who do not want this service in place must disconnect the USB modem from the MAS.

Chapter 8: Upgrading Modular Messaging software on an Avaya MAS

This chapter describes how to upgrade an Avaya MAS or a Supplementary server that is running Modular Messaging Release 3.0, Release 3.1, Release 4.0, or Release 5.1 software to Modular Messaging Release 5.2. In Modular Messaging Release 5.2, the process for upgrading an Avaya MAS and a Supplementary server is the same. You need to upgrade each MAS and then upgrade the Supplementary server.

If you are upgrading a customer-provided MAS, do not use the procedure in this chapter. See Upgrading Modular Messaging software on a customer-provided server on page 145.

CAUTION:

If you are upgrading to Exchange 2007 or Exchange 2010 or adding Exchange 2007 or Exchange 2010 mail servers, complete the upgrade to Modular Messaging Release 5.2 before you begin the Exchange 2007 or Exchange 2010 upgrade or additions. These are separate upgrade procedures and should not be completed concurrently.

Topics in this chapter include:

- Upgrading from Release 5.1 to Release 5.2 on page 124
- Upgrading from Release 3.x or Release 4.0 to Release 5.2 on page 125
- Upgrade requirements on page 125
- Preparing for the upgrade from Release 3.x or 4.0 on page 126
- Performing pre-upgrade tasks on page 128
- Upgrading Modular Messaging software on page 134
- Completing server setup on page 139
- Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 141

Upgrading from Release 5.1 to Release 5.2

To upgrade from Modular Messaging Release 5.1 to Release 5.2, you *must* use the latest Modular Messaging Release 5.2 Upgrade application available at the Avaya Support Web site (http://www.avaya.com/support).

Before you upgrade to Release 5.2, make sure that you:

- Obtain the *Upgrading MM components to Release 5.2 using Modular Messaging 5.2 Upgrade application* guide.
- Follow the instructions provided in the document to upgrade to Modular Messaging 5.2.
- *Do not* use the media to complete the upgrade. The procedure to upgrade Release 5.1 to Release 5.2 is different from the procedure you follow to upgrade from Modular Messaging Release 3.x or Release 4.0 to Release 5.2.

Upgrading from Release 3.x or Release 4.0 to Release 5.2

Perform the procedures provided in the following sections to upgrade Modular Messaging from Release 3.x or Release 4.0 to Release 5.2.

Upgrade requirements

To successfully upgrade a system to Modular Messaging Release 5.2, you need:

- Release 5.2 of the Modular Messaging application software and documentation:
  - *Avaya Modular Messaging Messaging Application Server Software* media. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
  - *Avaya Modular Messaging Documentation*.
- The planning forms or DCT used to install the existing Modular Messaging system.
- The following information and software from the Avaya Support Web site at http://www.avaya.com/support. For more information about how to access these items on the Web site, see Downloading required software and documentation on page 3.
  - The latest copy of the configuration notes for this switch integration.
  - Avaya software updates that are required to bring the Avaya Modular Messaging software up to date after an upgrade. Download this software to a USB storage device.
  - The latest copy of the DCT executable file (**MMDCT.exe**). Download the file from the Avaya support site to a USB storage device.
  - The latest Modular Messaging Client software package.
- A printed copy of the upgrade checklist for an Avaya MAS. See Modular Messaging upgrade on an Avaya MAS on page 236.
- WebLM server installed and configured. Use one of the following methods:
  - To install WebLM server on an MAS or a Supplementary server, proceed with Installing WebLM server on an MAS on page 90.
  - If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
  - To install WebLM server on a standalone server, see *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at http://www.avaya.com/support.

CAUTION:

For an upgrade from Release 3.x to Release 5.2: Release 5.2 does not support the following TTS engines: DecTalk and TTS3000. If you were using either of these TTS engines, the upgrade automatically removes them and installs the ScanSoft RealSpeak TTS engine.

- To ensure that the Modular Messaging system is at minimum Service Pack and Patch level.

Table 3: Minimum required Service Pack and patch level

MM Release Number	Minimum SP level required	Minimum Patch on SP required
3.0	SP7	Patch 4
3.1	Avaya does not recommend any specific SP or Patch level	
4.0	SP7	Patch 2

Prepare the server for the upgrade by running recommended disk checks. See Running recommended disk checks on page 133.

Preparing for the upgrade from Release 3.x or 4.0

Note:

A Modular Messaging software upgrade requires several server restarts. Plan to do the software upgrade during low-usage hours.

To upgrade the system to Modular Messaging Release 5.2:

1. Review the configuration notes for any changes that might be needed in the areas of board configuration, switch programming, and application configuration. For more information, see Upgrade requirements on page 125.
2. Complete pre-upgrade tasks to verify and save data, verify the DCT data file (*.*mmdct*), busy out ports, back up the MAS, run recommended disk checks, and stop and reset Modular Messaging services. For more information, see Performing pre-upgrade tasks on page 128.

   Note:

   When creating the DCT data file, include in the analysis any S3500 or S8730 MASs that will be replaced with S8800 1U MASs. Also include the supplementary server if one is present. A DCT data file is not required for the upgrade. However, create one prior to the upgrade to save important system information for backup.
3. Upgrade software on each MAS including: RealSpeak software and Modular Messaging software. For more information, see Upgrading Modular Messaging software on page 134.

4. Complete server setup by deleting old logs files, administering antivirus software, installing Modular Messaging software updates, updating Microsoft Windows, disabling the private LAN, and enabling ports.
5. Configure new Release 5.2 features and verify that required services are running.

   Note:

   Completely upgrade and test one MAS first, and let it run for 15 minutes before upgrading any additional MASs.
6. Update the Modular Messaging Subscriber Administration extensions on each MAS and any other computer where Modular Messaging was previously installed (such as administrator machines or the Exchange server). Update client software on client machines where it was previously installed. See detailed steps in Chapter 3: Adding Exchange extensions for Modular Messaging on page 37 and Updating client software on page 254.

   Note:

   Schedule downtime for the Microsoft Exchange server if the Modular Messaging Subscriber Administration extensions must be updated.
7. Perform acceptance tests on the entire system. See Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 141.
8. Back up the new data. See Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 141.

   CAUTION:

   All servers must meet the requirements listed in the *Avaya Modular Messaging Concepts and Planning Guide*. Review this document to verify that all Exchange servers, directory servers, MASs, and client machines are ready to support Modular Messaging software.

Considerations for multiple-MAS upgrades

In a multiple-MAS configuration, Avaya strongly recommends that all MASs that are running Release 3.x or 4.0 software be upgraded to Modular Messaging Release 5.2 software as soon as possible. During an upgrade MASs in the same Voice Mail Domain can run different releases of Modular Messaging. However, at the completion of an upgrade, all MASs in the Voice Mail Domain must be running Release 5.2.

All MASs in the voice mail domain must be upgraded to the same release of Modular Messaging software before you can enable the new Release 5.2 features.

Switching the monitor to show the correct server

You must switch the display from one server to another during a system upgrade.

For an 8-port Belkin KVM: the KVM switch is usually connected to the first Avaya MAS through the first computer port (VGA 01). Subsequent MASs (if present) are connected to computer ports VGA 02, VGA 03, and so on.

To show a different server on the monitor:

1. Gently press **Scroll Lock** twice and then press the up (or down) arrow key to change to the server connected to a higher (or lower) port number.

   Alternatively, type the port number using the keyboard. For example, type **1** for port 1.

2. If you cannot access the correct server, verify that the cable connections are correct. To correct cable problems, power down the system and correct the cable connections. Then turn on the system again.

For complete user and troubleshooting instructions, see the KVM switch documentation.

Performing pre-upgrade tasks

It is important that you record all critical system settings and back up all data in advance. Complete the following tasks to prepare the Modular Messaging system for an upgrade:

- Verifying and saving data on page 128
- Using the DCT to collect information from an MAS on page 130
- Busying out ports on page 132
- Backing up the MAS on page 132
- Running recommended disk checks on page 133
- Logging off all remote logins on page 133
- Stopping Modular Messaging services on page 133
- Applying Microsoft Windows Server 2003 Service Pack 2 on page 133
- Updating Windows Internet Explorer 7 security on page 134

Verifying and saving data

Complete the following tasks before you start a Release 5.2 upgrade:

1. Verify key settings on the MAS, including:
   - Switch integration settings
   - Port board settings and extensions
   - Domain information
   - Basic system setup
   - Modular Messaging service account and group

- Exchange settings

Make sure that you record the following items:

- Record the IP addresses for the MAS modems in the remote access service (RAS) group.
- In the VMSC for each MAS, record any *non-default* port groups and their names, such as the MWI port group.
- Record which Modular Messaging services are running on each MAS.
- Record the SNMP trap destination and community details from the **Serviceability — Voice Mail Domain** window.

2. For a Release 3.0 only, complete the following steps to record all personal operator schedules. This information will be required to verify the schedules following the upgrade.
   a. Click **Start > Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration**.
   b. Under the voice mail domain name, double-click **Telephone User Interface**.
   c. Select the **Personal Operator Schedules** tab.
   d. Click each schedule listed in the Schedules box and record the times set for each schedule.
   e. Close all windows.
3. On the MAS, disable alarms:
   a. Click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**.
   b. Under the voice mail domain name, double-click **Serviceability**.
   c. On the **Serviceability** page, on the **General** tab, select **Suppress alarm notifications**.
   d. Close all windows
4. If you use this MAS to create, administer and deploy caller applications, back up all your working files to a location other than the MAS. Additionally, on the MAS you must have a current backup of the Caller Apps folder that contains the deployed caller applications that the MAS uses when it is running. For example, you might have a backup of C:\Program Files\Avaya Modular Messaging\vserver\callerapps. Make a copy of the entire callerapps directory.
5. Review the configuration notes for any changes that might be needed regarding board configuration, switch programming, and application configuration. Verify configuration and make necessary changes as part of the upgrade.
6. Make a complete backup of all caller applications, customized tone files, customized prompt files, licensing files, WSO files and SIP certificates for SIP implementations. Also back up the system state and spool. See Backing up the system on page 119 for information about where to locate these files on your system.
7. Check for errors or warnings on the system. Resolve major and minor alarms.

8. Use the time estimates to set customer expectations for the time required to complete the upgrade.
9. Review product functionality with the customer, including:
    - Differences that will be noticeable to the customer
    - Known issues; see Product Support Notices (PSNs) on the Avaya support website
    - Rollout plan for new features
    - Security concerns

Using the DCT to collect information from an MAS

Use the Avaya Modular Messaging Data Collection Tool (DCT) to collect information from each MAS and Supplementary server.

Always check the Avaya Support Web site at http://www.avaya.com/support to obtain the most recent version of the DCT program. Download the mmdct.exe file to a storage device and use it instead of the one on the applications DVD. A DCT data file (*.mmdct) is not required for the upgrade. However, create a data file prior to the upgrade to save important system information for backup.

To create a DCT data file:

1. Verify that the Modular Messaging system is working properly. All MASs, the supplementary server, if present, and the Exchange message store must be running.
2. Switch the monitor to show MAS1. For more information, see Switching the monitor to show the correct server on page 127.
3. Log on using the customer account (for example, *mmacct*).
4. Verify that the messaging services on the MAS are running:
    a. Double-click the **Monitor** icon on the desktop or click **Start** > **Programs**> **Administration tools** > **Services**.
    b. In the left pane, click **Services (Local)**.
    c. In the right pane, scroll down to the list of Modular Messaging services. All services start with the abbreviation **MM**.
    d. Verify that the **Status** column shows that service is **Started** for each messaging service that belongs on this MAS.
    e. If service is not started for a required messaging service, right-click that **MM** service and select **Start**.
5. Insert the USB storage device with the DCT executable file (**MMDCT.exe**) into a USB port on MAS1. You can use any of the available USB ports.
6. Navigate to where you stored the executable file and double-click it.
7. On the **Select the DCT Configuration to use** screen, select **Analyze existing system**. Click **OK**.

8. When asked if you want to use an existing DCT data file (*.*mmdct*), click **No**.
9. On the **MM System Analysis** screen, select MAS#1 from the dropdown list at the bottom of the window. Click **Start**.

   The system displays the process of data collection. When analysis is complete, you see the message “information has been successfully collected,” The DCT displays the newly created DCT data file.
10. For a single-MAS upgrade, proceed to step 12. For a multiple-MAS system, save the DCT data file to a USB storage device.
11. For a multiple-MAS system, update the DCT data file with information from additional MASs and supplementary server:

    Note:

    Analyze all MASs in numeric order, first to last.

    a. Insert the USB storage device with the DCT data file created for MAS#1 into the USB port on the next MAS that you are going to analyze.

    b. Verify that the correct services are running on the MAS.

    c. On the USB storage device, double-click **MMDCT.exe**.

    d. On the **Select the DCT Configuration to use** screen, select **Analyze existing system**. Click **OK**.

    e. When asked if you want to use an existing DCT data file, click **Yes**.

    f. Navigate to where you saved the DCT data file that you created for MAS#1. Double-click it.

    g. In the **MM System Analysis** window, choose the number of the MAS that you are analyzing from the dropdown list at the bottom of the window. Click **Start**.

       The system displays the process of data collection. When analysis is complete, you see the message that information has been successfully collected. The DCT displays the newly updated file.

    h. Save the DCT data file by overwriting the previous file.

    CAUTION:

    In multiple-MAS systems, review and revise the DCT data file after analyzing all MASs that are to be upgraded. Information that is manually entered before the final analysis might be overwritten in the analysis of subsequent MASs.

    Do not change any data that was populated by the DCT system analysis.
12. Review the completed file. Enter information in empty fields if necessary.

Note:

Verify that there are no red **X**s next to the screen names in the left panel. Red x's indicate data that is incomplete or not valid. Information must be complete and valid before you can proceed with the upgrade. The DCT does not populate all fields when analyzing a system. It will be necessary to enter information, for example, passwords

13. When all fields in the DCT are complete, click **Complete** at the bottom of the screen. *S*ave the file to a location where it will be included in the backup. A DCT data file is not required for the upgrade. However, create one prior to the upgrade to save important system information for backup.

Busying out ports

Busy out the ports on the MAS that you are upgrading and on the switch before you start the upgrade. Otherwise, messages will spool on the MAS, and add to the upgrade time.

To busy out the ports:

1. The PBX administrator must use the procedures appropriate for this PBX to busy out the ports. Depending on the switch integration, the administrator might be able to temporarily reroute calls to other MASs. If an MAS is unavailable, callers into the system might hear ring-no answer or a busy signal.
2. Switch the monitor to show the MAS.
3. Use the port monitor to disable the MAS ports:
   a. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Port Monitor**.
   b. In the **Port Monitor** window, hold down the **Shift** key or Control (**Ctrl**) key and click to select all the ports.
   c. Right-click the port list and select **Disable**.
   d. Verify that the status of all ports is **Disabled**.
   e. Click **OK** to close this window.

Backing up the MAS

Before beginning the software upgrade, make a current backup of the important system files, including any customized tone files and the DCT data file that you just created. For this procedure, see Backing up the system on page 119.

CAUTION:

If any MAS backup fails to complete, *Do not* proceed with the upgrade. Contact your remote support center for assistance.

Running recommended disk checks

Avaya recommends that the hard disk drive in the server be maintained to prevent possible problems. Run the two following procedures if they were not previously run in preparation for the upgrade. See Upgrade requirements on page 125.

- Disk Defragmenter system tool
- **chkdsk** command

Logging off all remote logins

To log off all remote logins:

1. Log on to the MAS using an account that has administrative permissions.
2. Click **Start** > **Programs** > **Administration**.
3. Open your **Windows Task Manager** and select the **Users** tab.
4. Select remote logins and click **Logoff**.
5. If there are no remote logins, click **Cancel** to exit.

Stopping Modular Messaging services

Stop and reset all Modular Messaging (MM) services as follows:

Note:

If you have not already recorded the Modular Messaging services running on this MAS, do so now before stopping services.

1. Navigate to the **C:\Avaya_Support\tools\servicecontrol** directory.
2. Double-click the **StopMMServices.exe** file.

Applying Microsoft Windows Server 2003 Service Pack 2

All MASs in the Voice Mail Domain must be running Microsoft Windows Server 2003 Service Pack 2 for Modular Messaging Release 5.2. Install Microsoft Windows 2003 Service Pack 2 on this MAS. Check with the Windows administrator for site-specific procedures.

Updating Windows Internet Explorer 7 security

If your Avaya MAS has been upgraded to Internet Explorer 7 and if you are installing third-party software from a network drive complete the following steps to update Explorer 7 security. If you do not make this update and you use a domain account to install third-party software, Windows does not allow the installation. This procedure is not necessary if you are installing third-party software from a disk or other removable media such as a USB storage device.

1. Launch Windows Internet Explorer 7.
2. A window appears that states Windows Internet Explorer Enhanced Security is enabled; click **OK**.
3. From the browser, select **Tools** > **Internet Options**.
4. From the **Internet Options** window, select the **Security** tab.
5. In the **Select a zone to view or change security settings** box, click **Local intranet**.
6. Click **Sites**.
7. On the **Local intranet** window, click **Advanced**.
8. In the **Add this website to the zone** field, enter any one of the following:
   - *<drive letter>:*\, if you are using a mapped drive,
   - \\<*computername*>\<*share*\, if you are using a fully qualified domain name (FQDN) in the uniform naming convention (UNC) path,
   - the IP address, if you are specifying IP address in the UNC path.
9. Click **Add**.
10. Click **OK** to close the **Local intranet** window.
11. Click **OK** to close the **Internet Options** window.

Upgrading Modular Messaging software

Use the following procedures to upgrade from Release 3.x or 4.0 to Release 5.2:

- Upgrading Overnight on page 135
- Upgrading RealSpeak software on page 135
- Starting all Modular Messaging services on page 136
- Upgrading Dialogic drivers on page 136
- Upgrading MAS software on page 137

Upgrading Overnight

If you run the upgrade overnight, use the Voice Mail System Configuration application to disable the tracing database nightly tasks. After you complete the upgrade successfully, you must enable the scheduled tasks again when you perform the procedures in Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 141.

Upgrading RealSpeak software

Complete the following tasks *only* if you are upgrading from Release 3.x.

This section describes how to update the RealSpeak driver and languages as part of a Release 5.2 software upgrade.

To upgrade RealSpeak software, complete the following steps:

1. Log on to the MAS using the account that was originally used to install RealSpeak software. If you do not know which account was used, complete the following steps:
   a. Log on as the customer account (for example, *mmacct*).
   b. Click **Start** > **Control Panel** > **Add or Remove Programs.**
   c. In the list of currently installed programs, look for the **RealSpeak** program. If it is in the list continue with step 2 to delete the program.
   d. If the program was not in the list, repeat steps a through c with different accounts until you locate the RealSpeak program.
2. Insert the *Avaya Modular Messaging Messaging Application Server Software* (DVD **2** of **2**). You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
3. From the DVD, run the **RealSpeak\uninstallRealspeak.bat** file.
4. Reboot the MAS.
5. Log back on to the MAS using the account that was originally used to install RealSpeak software.
6. On the MAS, delete the folder **<*drive letter*>:\Program Files\ScanSoft**.
7. Verify that the *Avaya Modular Messaging Messaging Application Server Software* (DVD **2** of **2**) is in the DVD drive of the MAS.
8. In the media's **Realspeak** directory, double-click the **installRSEngine.bat** file.
9. Complete the wizard, accepting all defaults and the license agreement.
10. On **Ready to Install the Program**, click **Install**.
11. When installation is complete, click **Finish**.
12. Click **Yes** to restart the server.
13. Log back on to the MAS using the customer account.
14. In the **Realspeak** directory, double-click the **installRSLangs.bat** file.

15. After the RealSpeak languages are installed, remove the *Avaya Modular Messaging Messaging Application Server Software* media.

Starting all Modular Messaging services

Restart Modular Messaging services and verify that they are running:

1. Click **Start** > **Run** to open the **Run** window.
2. In the **Open** field, type the following and press **Enter**:

   C:\Avaya_Support\Scripts\serverrecovery.vbs

   The script takes a few seconds to run.
3. Verify that the services are set correctly.

Upgrading Dialogic drivers

Note:

You can skip this section, if your Modular Messaging server uses SIP based switch integration.

Do this task on each MAS that contains Dialogic port boards.

Complete these steps on any MAS that contains Dialogic port boards to update the drivers.

1. Log on to the MAS using the customer account (for example *mmacct*).
2. Insert the *Avaya Modular Messaging Messaging Application Server Software* media (disk **1** of **2**) in the DVD drive of the MAS. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
3. Uninstall Dialogic drivers:
   a. In the media's **\Dialogic Drivers** directory, double-click the **MMDialogicUninstall.bat** file.
   b. On the Question window, click **No**.
   c. On the Confirm Uninstall window, click **OK**.
   d. On the Maintenance Complete window, select **Yes, I want to restart my computer now** and then click **Finish**.
4. Log on to the MAS using the customer account.

   The **Clean-up Utility** runs automatically.
5. On the Hardware Update Wizard, click **Cancel**.
6. Reinstall Dialogic drivers:
   a. In the media's **\Dialogic Drivers** directory, double-click the **MMDialogicUpgrade.bat** file.

b. Complete the wizard, accepting all defaults.

c. If a warning window about Java appears, click **OK**.

A **Setup Status** window appears and installation begins.

After the Dialogic files install, a **Found New Hardware** window appears.

d. Select **No, not this time**, and click **Next**.

e. Select **Install the software automatically**, and click **Next**.

f. In the unsigned driver dialog box, click **Yes**.

g. After the board is set up, click **Finish**.

h. Repeat these steps for all Dialogic boards on this MAS.

i. On the Setup Complete window, select **Yes, I want to restart my computer now** and click **Finish**.

7. After the restart, log on to the MAS using the customer account.
8. From the media's **\Dialogic Drivers\mm_install** directory, double-click the **SetDialogicSettings.exe** file. This restores the Dialogic configuration to the MAS.
9. Start the Dialogic drivers:

a. Click **Start** > **Programs** > **Intel Dialogic System Release** > **Configuration Manager - DCM**.

The system displays the Intel Dialogic product **Configuration Manager** window.

b. On the button bar, click the green **> (Start)** button.

Wait for the devices to start and the installed boards to show a green light.

c. Close the **DCM** window.

10. Reboot the MAS.

Upgrading MAS software

Note:

If antivirus software is installed, Avaya recommends that you disable it while you upgrade the Modular Messaging software to prevent possible negative interactions. Enable the virus-checking software again after the upgrade is complete.

To upgrade the software on this MAS to Modular Messaging Release 5.2:

1. If you changed any logging settings before the upgrade, complete the following steps:

a. Launch **c:\avaya_support\tools\MM_Logging\MMLogging.exe**.

b. Record any values that you changed, such as **Log file size** and **Number of log files**.

2. Close all monitoring tools, such as the port monitor.

3. Log on to the MAS using the customer account (for example *mmacct*).
4. Insert the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1) in the DVD drive of the MAS. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
5. In the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1) **Install** directory, double-click the **Setup.exe** file.

   The system launches the Avaya Modular Messaging Installation Wizard. All components that were previously installed on this machine, and the Diagnostic tools, are automatically selected. These selections cannot be changed. The currently installed version is displayed to the right of the specific tool or application. The version that is to be installed is displayed at the top of the page following the Avaya Modular Messaging title.

   a. Verify that the **Select Configuration** field displays **Microsoft Exchange**.
   b. For all upgrades check the following boxes:
      - **Enable Windows Installer logging**
      - **Fax Sender Server**
   c. For Release 3.x or Release 4.0 to Release 5.2 upgrades also select the following check boxes:
      - **MM Configuration Tools**
      - **Snapshot Utility**
      - **Web Subscriber Options User Interface**
      - Any additional components that are necessary for this MAS
   d. Click **Install**.
   e. Click **Run System Upgrade**.
   f. When prompted, click **Restart** to continue the upgrade.
6. When the restart is complete, log on as the Modular Messaging customer account (such as *mmacct*).

   The Installation Wizard starts automatically. If the wizard does not automatically start, double-click the **Setup.exe** file.
7. Follow prompts to remove service packs and patches as needed. Depending on the patch, if the system requests it, restart the server.

   The system upgrades the Modular Messaging software components. This step can take several minutes.
8. If prompted by the system, enter the password of the account used by Modular Messaging services.
9. Follow the installation Configuration Wizard prompts.

   The system upgrades the Modular Messaging software components. The components window shows which component is being installed. The system pauses for several minutes

when installing the Avaya SPIRIT Agent. This is normal. Also, this step might take several minutes for a large database or a global address list (GAL).

10. If you installed Web Subscriber Options, follow the prompts to complete the installation wizard.
11. When the Installation Wizard flashes a warning that installation is not complete, restart the system and log back on as the Modular Messaging customer account (such as *mmacct*).

    The Installation Configuration Wizard runs automatically displaying the Service Configuration window.
12. When the update is complete, click **Finish**.
13. Remove the media from the DVD drive.
14. Verify the settings of the MM Services. If any are incorrect, reset them to the correct setting.
15. If you disabled the antivirus software on this MAS, enable it again now.

Completing server setup

- Verifying antivirus software on page 139
- Installing software updates on page 140
- Updating Microsoft Windows on page 140
- Enabling ports on page 140
- Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 141
- Updating client software on page 254

Verifying antivirus software

Avaya strongly recommends that antivirus software be installed on any Microsoft Windows computer that runs Avaya Modular Messaging software. The type of virus-checking software used and the method of installation depends on customer requirements and the local implementation. Verify that the MAS is running the latest version of the antivirus software. For additional guidelines for configuring antivirus software, see Administering antivirus software on page 54.

Installing and configuring WebLM server

Install and configure the WebLM server. Use one of the following methods:

- To install WebLM server on an MAS or a Supplementary server, proceed with Installing WebLM server on an MAS on page 90.

- If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
- To install WebLM server on a standalone server, see *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at http://www.avaya.com/support.

Installing software updates

A new Modular Messaging system ships with the most current software that is available at the time. However, the software must be updated after an upgrade to include the latest changes. The updates might be in the form of an Avaya Service Pack (SP) or a software patch (hot fix).

To determine if a Modular Messaging software update is needed:

1. Locate any relevant Avaya software updates on the Avaya Support Web site at http://www.avaya.com/support. For complete steps, see Obtaining software updates from the Web on page 303.

   Note:

   If you followed the procedure for Downloading software updates on page 4, you already downloaded any required software updates.

2. If the Modular Messaging system requires a software update, complete the update procedure now before you do acceptance testing. Follow the instructions in Appendix E: Updating Modular Messaging software on page 303 to update the system with the latest changes.

Updating Microsoft Windows

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

Note:

Avaya technical support representatives must follow their specified internal procedures for verifying the software that is installed. If required, they must update the software with the latest patches as instructed.

Enabling ports

Enable the ports on the MAS that you are upgrading.

Use the port monitor to enable the MAS ports:

1. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Port Monitor**.

2. In the **Port Monitor** window, hold down the **Shift** key or Control (**Ctrl**) key and click to select all the ports.
3. Right-click the port list and select **Enable**.
4. Verify that the status of all ports is **Enabled**.
5. Close the **Port Monitor** window

Completing the Release 3.x or 4.0 to Release 5.2 upgrade

This section describes the topics required to complete the upgrade of the Modular Messaging system to Release 5.2.

Continue the Modular Messaging software upgrade as appropriate:

1. Install and configure the WebLM server. Use one of the following methods:
   - To install WebLM server on an MAS or a Supplementary server, proceed with Installing WebLM server on an MAS on page 90.
   - If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
   - To install WebLM server on a standalone server, see *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at http://www.avaya.com/support.
2. If you have more than one MAS:
   a. ***For the first MAS upgraded only,*** let the Modular Messaging software run for 15 minutes. Return to Switching the monitor to show the correct server on page 127 to begin upgrading the next MAS.
   b. Repeat the Modular Messaging software upgrade procedure until all MASs are upgraded.

   CAUTION:
   Perform steps 3 and 4 only if you are upgrading from Release 3.x to Release 5.2.
3. Enable and configure MM Fax Service. If this MAS is to run the MM Fax Sender Service, complete the following steps:
   a. Navigate to the **C:\Avaya_Support\Utils** directory.
   b. Double-click the **FaxSenderEnable.exe** file.
   c. Restart Microsoft Windows Fax Service.
   d. Configure MM Fax Service by completing the steps described in Configuring the MM Fax Sender server on page 96.

Note:

The dual span QSIG boards require configuration of the **FirmwareFile 2** parameter on the **Intel Dialogic product Configuration Manager - Properties** window. For more information, see Configuring T1-QSIG or E1-QSIG boards on page 310.

4. Configure Audit service by completing the steps described in Configuring Audit Service on page 96.
5. Configure and activate additional new Release 5.2 features as needed using the Voice Mail System Configuration program.
6. Enable all scheduled tasks that you disabled before starting the upgrade.
7. Update the Modular Messaging Active Directory Exchange extensions on machines where they are installed. See Chapter 3: Adding Exchange extensions for Modular Messaging on page 37.

   Note:

   The Modular Messaging Active Directory Exchange extensions are updated along with other Modular Messaging software that is installed on this machine (multiple Modular Messaging software component check boxes might be selected). This ensures that all currently installed components are upgraded. The components are installed in the correct order when you click **Install**.
8. Update the client software on non-MAS machines where it is installed. See Updating client software on page 254.
9. When finished with each MAS, verify that the MAS disk is in good condition by running the following:
   - Disk Defragmenter system tool
   - **chkdsk** command
10. Do the acceptance tests that are appropriate for each server; see Performing acceptance tests on page 112. For example:
    a. For an MAS, test to check if the server can send and receive calls.
    b. For all servers, verify that the services run on the appropriate server.
11. Run a DCT analyze on the system; see Using the DCT to collect information from an MAS on page 130.
12. Complete the following steps to verify all Personal Operator Schedules:
    a. Click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**.
    b. Under the voice mail domain name, double-click **Telephone User Interface**.
    c. Select the **Personal Operator Schedules** tab.
    d. Verify that all Personal Operator Schedules recorded before the upgrade are included in the list. If a schedule is missing, complete the following steps:

1. Click the **Add** button
2. In the **Enter Personal Operator Schedule Name** dialog box in the **Schedule Name** field, enter the name of the missing schedule.
3. Click **OK** to return to the Personal Operator Schedules tab.
4. In the schedule grid, enter the schedule times.

e. Click each Personal Operator Schedule in the schedule list and verify that the schedule times correspond to the times recorded before the upgrade. Correct discrepancies in the schedule grid.

f. Close all windows.

13. Review event and alarm logs and resolve problems; obtain the *Avaya Modular Messaging MAS Administration Guide*; see Downloading user documentation on page 5.
14. Run backups on each MAS; see Backing up the MAS on page 132.
15. Perform this step *only* if you are upgrading from Release 3.x. Due to a change in file names, old logs might remain on the system. Remove old logs from ***c:\avaya_support\logs*** folder on each MAS and delete logs that are older than the upgrade's start time.
16. On the MAS, enable alarms:

    a. Configure the SNMP trap destination and community details using the **Serviceability - Voice Mail Domain** window of the Voice Mail System Configuration program. Enter the SNMP trap destination and community information you recorded before beginning the upgrade.

    b. Click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**.

    c. Under the voice mail domain name, double-click **Serviceability**.

    d. On the **Serviceability** page, on the **General** tab, clear the **Suppress alarm notifications** check box, to turn on the alarm notifications options.

    e. Click **Save** to save the changes.

    f. Close all windows.

17. If you are adding a new MAS to this system, begin the installation now. For more information, see *Installing the Avaya S8800 Server for Modular Messaging*.

For post-install procedure of. the MAS,
see Post-installation procedures for Modular Messaging on page 253

Chapter 9: Upgrading Modular Messaging software on a customer-provided server

This chapter describes how to upgrade a customer-provided MAS or supplementary server that is running Modular Messaging Release 3.x, Release 4.0, or Release 5.1 software to Modular Messaging Release 5.2.

If you are upgrading an Avaya MAS, do not use the procedure in this chapter. See Upgrading Modular Messaging software on an Avaya MAS on page 123

If you are changing the switch integration, perform the procedure before or after you complete the upgrade process. For more information on how to change the switch integration, see Changing switch integration on page 269.

CAUTION:

If you are upgrading to Exchange 2007 or Exchange 2010 or adding Exchange 2007 or Exchange 2010 mail servers, complete the upgrade to Modular Messaging Release 5.2 before you begin the Exchange 2007 or Exchange 2010 upgrade or additions. These are separate upgrade procedures and should not be completed concurrently.

Topics in this chapter include:

- Upgrading from Release 5.1 to Release 5.2 on page 146

Upgrading from Release 3.x or Release 4.0:

- Upgrade requirements on page 147
- Preparing for the upgrade from Release 3.x or 4.0 on page 149
- Performing pre-upgrade tasks on page 150
- Upgrading Modular Messaging software on page 158
- Completing server setup on page 163
- Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 165

Upgrading from Release 5.1 to Release 5.2

To upgrade from Modular Messaging Release 5.1 to Release 5.2, you *must* use the latest Modular Messaging Release 5.2 Upgrade application available at the Avaya Support Web site (http://www.avaya.com/support).

Before you upgrade to Release 5.2, make sure that you:

- Obtain the *Upgrading MM components to Release 5.2 using Modular Messaging 5.2 Upgrade application* guide.
- Follow the instructions provided in the document to upgrade to Modular Messaging Release 5.2.
- *Do not* use the media to complete the upgrade. The procedure to upgrade Release 5.1 to Release 5.2 is different from the procedure you follow to upgrade from Modular Messaging Release 3.x or Release 4.0 to Release 5.2.

Upgrade requirements

To successfully upgrade a system to Modular Messaging Release 5.2, you need:

- Release 5.2 of the Modular Messaging application software and documentation:
  - *Avaya Modular Messaging Messaging Application Server Software* media. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
  - *Avaya Modular Messaging Documentation*.
- The planning forms or DCT file used to install the existing Modular Messaging system.
- The following information and software from the Avaya Support Web site at http://www.avaya.com/support. For more information about how to access these items on the Web site, see Downloading required software and documentation on page 3.
  - The latest copy of the configuration notes for this switch integration.
  - Avaya software updates that are required to bring the Avaya Modular Messaging software up to date after an upgrade. Download this software to a USB storage device.
  - The latest copy of the DCT executable file (**MMDCT.exe**). Download the file from the Avaya support site to a USB storage device.
  - The latest Modular Messaging Client software package.
- A printed copy of the upgrade checklist for a customer-provided MAS. See Modular Messaging upgrade on an Avaya MAS on page 236.
- WebLM server installed and configured. Use one of the following methods:
  - To install WebLM server on an MAS or a Supplementary server, proceed with Installing WebLM server on an MAS on page 90.
  - If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
  - To install WebLM server on a standalone server, see *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at http://www.avaya.com/support.

CAUTION:

For an upgrade from Release 3.x to Release 5.2: Release 5.2 does not support the following TTS engines: DecTalk and TTS3000. If you were using either of these TTS engines, the upgrade automatically removes them and installs the ScanSoft RealSpeak TTS engine.

- To ensure that the Modular Messaging system is at minimum Service Pack and Patch level. For more information, see Minimum required Service Pack and patch level on page 148.

Table 4: Minimum required Service Pack and patch level

MM Release Number	Minimum SP level required	Minimum Patch on SP required
3.0	SP7	Patch 4
3.1	Avaya does not recommend any specific SP or Patch level	
4.0	SP7	Patch 2

Prepare the server for the upgrade by running recommended disk checks. See Running recommended disk checks on page 155.

Preparing for the upgrade from Release 3.x or 4.0

Note:

A Modular Messaging software upgrade requires several server restarts. Plan to do the software upgrade during low-usage hours.

To upgrade the system to Modular Messaging Release 5.2:

1. Review the configuration notes for any changes that might be needed in the areas of board configuration, switch programming, and application configuration. For more information, see Upgrade requirements on page 147.
2. Complete pre-upgrade tasks to verify and save data, verify the DCT data file (**.mmdct*), busy out ports, back up the MAS, run recommended disk checks, and stop and reset Modular Messaging services.
3. Upgrade software on each MAS including: RealSpeak software, and Modular Messaging software. For more information, see Upgrading Modular Messaging software on page 158.
4. Complete server setup by deleting old logs files, administering antivirus software, installing Modular Messaging software updates, updating Microsoft Windows, disabling the private LAN, and enabling ports.
5. Configure new Release 5.2 features and verify that required services are running.

   Note:

   Completely upgrade and test one MAS first, and let it run for 15 minutes before upgrading any additional MASs.
6. Update the Modular Messaging Subscriber Administration extensions on each MAS and any other computer where Modular Messaging was previously installed (such as administrator machines or the Exchange server). Update client software on client machines where it was previously installed. See detailed steps in Chapter 3: Adding Exchange extensions for Modular Messaging on page 37 and Updating client software on page 254.

   Note:

   Schedule downtime for the Microsoft Exchange server if the Modular Messaging Subscriber Administration extensions must be updated.
7. Perform acceptance tests on the entire system. See Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 165.
8. Back up the new data. See Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 165.

CAUTION:

All servers must meet the requirements listed in the *Avaya Modular Messaging Concepts and Planning Guide*. Review this document to verify that all Exchange servers, directory servers, MASs, and client machines are ready to support Modular Messaging software.

Considerations for multiple-MAS upgrades

In a multiple-MAS configuration, Avaya strongly recommends that all MASs that are running Release 3.x or 4.0 software be upgraded to Modular Messaging Release 5.2 software as soon as possible. During an upgrade MASs in the same Voice Mail Domain can run different releases of Modular Messaging. However, at the completion of an upgrade, all MASs in the Voice Mail Domain must be running Release 5.2.

All MASs in the voice mail domain must be upgraded to the same release of Modular Messaging software before you can enable the new Release 5.2 features.

Switching the monitor to show the correct server

You must switch the display from one server to another during a system upgrade.

To show a different server on the monitor:

1. Gently press **Scroll Lock** twice and then press the up (or down) arrow key to change to the server connected to a higher (or lower) port number.

   Alternatively, type the port number using the keyboard. For example, type **1** for port 1.

2. If you cannot access the correct server, verify that the cable connections are correct. To correct cable problems, power down the system and correct the cable connections. Then turn on the system again.

For complete user and troubleshooting instructions, see the KVM switch documentation.

Performing pre-upgrade tasks

It is important that you record all critical system settings and back up all data in advance. Complete the following tasks to prepare the Modular Messaging system for an upgrade:

- Verifying and saving data on page 151
- Using the DCT to collect information from an MAS on page 152
- Busying out ports on page 154

- Backing up the MAS on page 155
- Running recommended disk checks on page 155
- Logging off all remote logins on page 155
- Stopping Modular Messaging services on page 156
- Installing Microsoft Windows prerequisite components on page 156
- Applying Microsoft Windows Server 2003 Service Pack 2 on page 156
- Updating Windows Internet Explorer 7 security on page 157

Verifying and saving data

Complete the following tasks before you start a Release 5.2 upgrade:

1. Verify key settings on the MAS, including:
   - Switch integration settings
   - Port board settings and extensions
   - Domain information
   - Basic system setup
   - Modular Messaging service account and group
   - Exchange settings

   Ensure that you record the following items:
   - Record the IP addresses for the MAS modems in the remote access service (RAS) group.
   - In the VMSC for each MAS, record any *non-default* port groups and their names, such as the MWI port group.
   - Record which Modular Messaging services are running on each MAS.
   - Record the SNMP trap destination and community details from the **Serviceability — Voice Mail Domain** window.
2. For a Release 3.0 only, complete the following steps to record all personal operator schedules. This information will be required to verify the schedules following the upgrade.
   a. Click **Start > Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration**.
   b. Under the voice mail domain name, double-click **Telephone User Interface**.
   c. Select the **Personal Operator Schedules** tab.
   d. Click each schedule listed in the Schedules box and record the times set for each schedule.

e. Close all windows.

3. On the MAS, disable alarms:
   a. Click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**.
   b. Under the voice mail domain name, double-click **Serviceability**.
   c. On the **Serviceability** page, on the **General** tab, select **Suppress alarm notifications**.
   d. Close all windows
4. If you use this MAS to create, administer and deploy caller applications, back up all your working files to a location other than the MAS. Additionally, on the MAS you must have a current backup of the Caller Apps folder that contains the deployed caller applications that the MAS uses when it is running. For example, you might have a backup of **C:\Program Files\Avaya Modular Messaging\vserver\callerapps**. Make a copy of the entire callerapps directory.
5. Review the configuration notes for any changes that might be needed regarding board configuration, switch programming, and application configuration. Verify configuration and make necessary changes as part of the upgrade.
6. Make a complete backup of all caller applications, customized tone files, customized prompt files, licensing files, WSO files and SIP certificates for SIP implementations. Also back up the system state and spool. See Backing up the system on page 119 for information about where to locate these files on your system.
7. Check for errors or warnings on the system. Resolve major and minor alarms.
8. Use the time estimates to set customer expectations for the time required to complete the upgrade.
9. Review product functionality with the customer, including:
   - Differences that will be noticeable to the customer
   - Known issues; see Product Support Notices (PSNs) on the Avaya support website
   - Rollout plan for new features
   - Security concerns

Using the DCT to collect information from an MAS

Use the Avaya Modular Messaging Data Collection Tool (DCT) to collect information from each MAS and Supplementary server.

Always check the Avaya Support Web site at http://www.avaya.com/support to obtain the most recent version of the DCT program. Download the mmdct.exe file to a storage device and use it instead of the one on the applications DVD. A DCT data file (*.*mmdct*) is not required for the

upgrade. However, create a data file prior to the upgrade to save important system information for backup.

To create a DCT data file:

1. Verify that the Modular Messaging system is working properly. All MASs, the supplementary server, if present, and the Exchange message store must be running.
2. Switch the monitor to show MAS1. For more information, see Switching the monitor to show the correct server on page 150.
3. Log on using the customer account (for example, *mmacct*).
4. Verify that the messaging services on the MAS are running:
   a. Double-click the **Monitor** icon on the desktop or click **Start** > **Programs**> **Administration tools** > **Services**.
   b. In the left pane, click **Services (Local)**.
   c. In the right pane, scroll down to the list of Modular Messaging services. All services start with the abbreviation **MM**.
   d. Verify that the **Status** column shows that service is **Started** for each messaging service that belongs on this MAS.
   e. If service is not started for a required messaging service, right-click that **MM** service and select **Start**.
5. Insert the USB storage device with the DCT executable file (**MMDCT.exe**) into a USB port on MAS1. You can use any of the available USB ports.
6. Navigate to where you stored the executable file and double-click it.
7. On the **Select the DCT Configuration to use** screen, select **Analyze existing system**. Click **OK**.
8. When asked if you want to use an existing DCT data file (**.mmdct*), click **No**.
9. On the **MM System Analysis** screen, select MAS#1 from the dropdown list at the bottom of the window. Click **Start**.

   The system displays the process of data collection. When analysis is complete, you see the message “information has been successfully collected,” The DCT displays the newly created DCT data file.
10. For a single-MAS upgrade, proceed to step 12. For a multiple-MAS system, save the DCT data file to a USB storage device.
11. For a multiple-MAS system, update the DCT data file with information from additional MASs:

    Note:

    Analyze all MASs in numeric order, first to last.

    a. Insert the USB storage device with the DCT data file created for MAS#1 into the USB port on the next MAS that you are going to analyze.

b. Verify that the correct services are running on the MAS.

c. On the USB storage device, double-click **MMDCT.exe**.

d. On the **Select the DCT Configuration to use** screen, select **Analyze existing system**. Click **OK**.

e. When asked if you want to use an existing DCT data file, click **Yes**.

f. Navigate to where you saved the DCT data file that you created for MAS#1. Double-click it.

g. In the **MM System Analysis** window, choose the number of the MAS that you are analyzing from the dropdown list at the bottom of the window. Click **Start**.

The system displays the process of data collection. When analysis is complete, you see the message that information has been successfully collected. The DCT displays the newly updated file.

h. Save the DCT data file by overwriting the previous file.

CAUTION:

In multiple-MAS systems, review and revise the DCT data file after analyzing all MASs that are to be upgraded. Information that is manually entered before the final analysis might be overwritten in the analysis of subsequent MASs.

Do not change any data that was populated by the DCT system analysis.

12. Review the completed file. Enter information in empty fields if necessary.

Note:

Verify that there are no red **X**s next to the screen names in the left panel. Red **x**'s indicate data that is incomplete or not valid. Information must be complete and valid before you can proceed with the upgrade. The DCT does not populate all fields when analyzing a system. It will be necessary to enter information, for example, passwords

13. When all fields in the DCT are complete, click **Complete** at the bottom of the screen. *S*ave the file to a location where it will be included in the backup. A DCT data file is not required for the upgrade. However, create one prior to the upgrade to save important system information for backup.

Busying out ports

Busy out the ports on the MAS that you are upgrading and on the switch before you start the upgrade. Otherwise, messages will spool on the MAS, and add to the upgrade time.

To busy out the ports:

1. The PBX administrator must use the procedures appropriate for this PBX to busy out the ports. Depending on the switch integration, the administrator might be able to temporarily

reroute calls to other MASs. If an MAS is unavailable, callers into the system might hear ring-no answer or a busy signal.

2. Switch the monitor to show the MAS.
3. Use the port monitor to disable the MAS ports:
   a. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Port Monitor**.
   b. In the **Port Monitor** window, hold down the **Shift** key or Control (**Ctrl**) key and click to select all the ports.
   c. Right-click the port list and select **Disable**.
   d. Verify that the status of all ports is **Disabled**.
   e. Click **OK** to close this window.

Backing up the MAS

Before beginning the software upgrade, make a current backup of the important system files, including any customized tone files and the DCT data file that you just created. For this procedure, see Backing up the system on page 119.

CAUTION:
If any MAS backup fails to complete, *Do not* proceed with the upgrade. Contact your remote support center for assistance.

Running recommended disk checks

Avaya recommends that the hard disk drive in the server be maintained to prevent possible problems. Run the two following procedures if they were not previously run in preparation for the upgrade. See Upgrade requirements on page 147.

- Disk Defragmenter system tool
- **chkdsk** command

Logging off all remote logins

To log off all remote logins:

1. Log on to the MAS using an account that has administrative permissions.
2. Click **Start** > **Programs** > **Administration**.
3. Open your **Windows Task Manager** and select the **Users** tab.

4. Select remote logins and click **Logoff**.
5. If there are no remote logins, click **Cancel** to exit.

Stopping Modular Messaging services

Stop and reset all Modular Messaging (MM) services as follows:

Note:

If you have not already recorded the Modular Messaging services running on this MAS, do so now before stopping services.

1. Navigate to the **C:\Avaya_Support\tools\servicecontrol** directory.
2. Double-click the **StopMMServices.exe** file.

Installing Microsoft Windows prerequisite components

Complete the following steps to install Microsoft Windows prerequisite components on the MAS only if you are upgrading from Modular Messaging Release 3.x.

1. Insert the Microsoft Windows operating system installation disk in the MAS DVD drive.
2. Click **Start** > **Control Panel** > **Add or Remove Programs**.
3. In the **Add or Remove Programs** window, in the left column, click **Add/Remove Windows Components**.
4. In the **Windows Components Wizard** window, highlight **Application Server** and click **Details**.
5. Select the **Message Queuing** check box and press **OK**.
6. in the **Windows Components Wizard** window, select the **Fax Services** check box and click **Next**.
7. Select **Do Not Share Fax Printer** and click **Next**.
8. When installation is complete, click **Finish**.
9. Verify that fax service is **Started** and set to **Automatic**.

Applying Microsoft Windows Server 2003 Service Pack 2

All MASs in the Voice Mail Domain must be running Microsoft Windows Server 2003 Service Pack 2 for Modular Messaging Release 5.2. Install Microsoft Windows 2003 Service Pack 2 on this MAS. Check with the Windows administrator for site-specific procedures.

Updating Windows Internet Explorer 7 security

If your MAS has been upgraded to Internet Explorer 7 and if you are installing third-party software from a network drive complete the following steps to update Explorer 7 security. If you do not make this update and you use a domain account to install third-party software, Windows does not allow the installation. This procedure is not necessary if you are installing third-party software from a disk or other removable media such as a USB storage device.

1. Launch Windows Internet Explorer 7.
2. A window appears that states Windows Internet Explorer Enhanced Security is enabled; click **OK**.
3. From the browser, select **Tools** > **Internet Options**.
4. From the **Internet Options** window, select the **Security** tab.
5. In the **Select a zone to view or change security settings** box, click **Local intranet**.
6. Click **Sites**.
7. On the **Local intranet** window, click **Advanced**.
8. In the **Add this website to the zone** field, enter any one of the following:
   - <*drive letter*>:\, if you are using a mapped drive,
   - \\<*computername*>\<*share*\, if you are using a fully qualified domain name (FQDN) in the uniform naming convention (UNC) path,
   - the IP address, if you are specifying IP address in the UNC path.
9. Click **Add**.
10. Click **OK** to close the **Local intranet** window.
11. Click **OK** to close the **Internet Options** window.

Upgrading Modular Messaging software

Use the following procedures to upgrade from Release 3.x or 4.0 to Release 5.2

- Upgrading Overnight on page 158
- Upgrading RealSpeak software on page 158
- Starting all Modular Messaging services on page 159
- Upgrading Dialogic drivers on page 159
- Upgrading MAS software on page 161

Upgrading Overnight

If you run the upgrade overnight, use the Voice Mail System Configuration application to disable the tracing database nightly tasks. After you complete the upgrade successfully, you must enable the scheduled tasks again when you perform the procedures in Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 165.

Upgrading RealSpeak software

Complete the following tasks *only* if you are upgrading from Release 3.x.

This section describes how to update the RealSpeak driver and languages as part of a Release 5.2 software upgrade.

To upgrade RealSpeak software, complete the following steps:

1. Log on to the MAS using the account that was originally used to install RealSpeak software. If you do not know which account was used, complete the following steps:
   a. Log on as the customer account (for example, *mmacct*).
   b. Click **Start** > **Control Panel** > **Add or Remove Programs.**
   c. In the list of currently installed programs, look for the **RealSpeak** program. If it is in the list, continue with step 2 to delete the program.
   d. If the program is not in the list, repeat steps a through c with different accounts until you locate the RealSpeak program.
2. Insert the *Avaya Modular Messaging Messaging Application Server Software* (DVD **2** of **2**). You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
3. From the DVD, run the **RealSpeak\uninstallRealspeak.bat** file.

   The MAS restarts.
4. Log on to the MAS using the account that was originally used to install RealSpeak software.
5. On the MAS, delete the folder **<*drive letter*>:\Program Files\ScanSoft**.

6. Verify that the *Avaya Modular Messaging Messaging Application Server Software* (DVD **2** of **2**) is in the DVD drive of the MAS.
7. In the media's **Realspeak** directory, double-click the **installRSEngine.bat** file.
8. Complete the wizard, accepting all defaults and the license agreement.
9. On **Ready to Install the Program**, click **Install**.
10. When installation is complete, click **Finish**.
11. Click **Yes** to restart the server.
12. Log back on to the MAS using the customer account.
13. In the **Realspeak** directory, double-click the **installRSLangs.bat** file.
14. After the RealSpeak languages are installed, remove the *Avaya Modular Messaging Messaging Application Server Software* media.

Starting all Modular Messaging services

Restart Modular Messaging services and verify that they are running:

1. Click **Start** > **Run** to open the **Run** window.
2. In the **Open** field, type the following and press **Enter**:

   C:\Avaya_Support\Scripts\serverrecovery.vbs

   The script takes a few seconds to run.
3. Verify that the services are set correctly.

Upgrading Dialogic drivers

Note:

You can skip this section, if your Modular Messaging server uses SIP based switch integration.

Do this task on each MAS that contains Dialogic port boards.

Complete these steps on any MAS that contains Dialogic port boards to update the drivers.

1. Log on to the MAS using the customer account (for example *mmacct*).
2. Insert the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1) in the DVD drive of the MAS. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
3. Uninstall Dialogic drivers:
   a. In the media's **\Dialogic Drivers** directory, double-click the **MMDialogicUninstall.bat** file.
   b. On the **Question** window, click **No**.

c. On the **Confirm Uninstall** window, click **OK**.

d. On the **Maintenance Complete** window, select **Yes, I want to restart my computer now** and then click **Finish**.

4. Log on to the MAS using the customer account.

   The **Clean-up Utility** runs automatically.

5. On the **Hardware Update Wizard**, click **Cancel**.

6. Reinstall Dialogic drivers:

   a. In the media's **\Dialogic Drivers** directory, double-click the **MMDialogicUpgrade.bat** file.

   b. Complete the wizard, accepting all defaults.

   c. If a warning window about Java appears, click **OK**.

      A **Setup Status** window appears and installation begins.

      After the Dialogic files install, a **Found New Hardware** window appears.

   d. Select **No, not this time**, and click **Next**.

   e. Select **Install the software automatically**, and click **Next**.

   f. In the unsigned driver dialog box, click **Yes**.

   g. After the board is set up, click **Finish**.

   h. Repeat these steps for all Dialogic boards on this MAS.

   i. On the Setup Complete window, select **Yes, I want to restart my computer now** and click **Finish**.

7. After the restart, log on to the MAS using the customer account.

8. From the media's **\Dialogic Drivers\mm_install** directory, double-click the **SetDialogicSettings.exe** file. This restores the Dialogic configuration to the MAS.

9. Start the Dialogic drivers:

   a. Click **Start** > **Programs** > **Intel Dialogic System Release** > **Configuration Manager - DCM**.

      The system displays the Intel Dialogic product **Configuration Manager** window.

   b. On the button bar, click the green **> (Start)** button.

      Wait for the devices to start and the installed boards to show a green light.

   c. Close the **DCM** window.

10. Reboot the MAS.

Upgrading MAS software

Note:

If antivirus software is installed, Avaya recommends that you disable it while you upgrade the Modular Messaging software to prevent possible negative interactions. Enable the virus-checking software again after the upgrade is complete.

To upgrade the software on this MAS to Modular Messaging Release 5.2:

1. If you changed any logging settings before the upgrade, complete the following steps:
   a. Launch **c:\avaya_support\tools\MM_Logging\MMLogging.exe**.
   b. Record any values that you changed, such as **Log file size** and **Number of log files**.
2. Close all monitoring tools, such as the port monitor.
3. Log on to the MAS using the customer account (for example *mmacct*).
4. Insert the *Avaya Modular Messaging Messaging Application Server Software* media (disk **1** of **2**) in the DVD drive of the MAS. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
5. In the *Avaya Modular Messaging Messaging Application Server Software* media (disk **1** of **2**) **Install** directory, double-click the **Setup.exe** file.

   The system launches the Avaya Modular Messaging Installation Wizard. All components that were previously installed on this machine, and the Diagnostic tools, are automatically selected. These selections cannot be changed. The currently installed version is displayed to the right of the specific tool or application. The version that is to be installed is displayed at the top of the page following the Avaya Modular Messaging title.

   a. Verify that the **Select Configuration** field displays **Microsoft Exchange**.
   b. For all upgrades check the following boxes:
      - **Enable Windows Installer logging**
      - **Fax Sender Server**
   c. For Release 3.x or Release 4.0 to Release 5.2 upgrades also select the following check boxes:
      - **MM Configuration Tools**
      - **Snapshot Utility**
      - **Web Subscriber Options User Interface**
      - Any additional components that are necessary for this MAS
   d. Click **Install**.
   e. Click **Run System Upgrade**.

f. When prompted, click **Restart** to continue the upgrade.

   If the system fails to restart, a message box appears.

g. Click **Terminate the process**.

6. When the restart is complete, log on as the Modular Messaging customer account (such as *mmacct*).

   The Installation Wizard starts automatically. If the wizard does not automatically start, double-click the **Setup.exe** file.

7. Follow prompts to remove service packs and patches as needed. Depending on the patch, if the system requests it, restart the server.

   The system upgrades the Modular Messaging software components. This step can take several minutes.

8. If prompted by the system, enter the password of the account used by Modular Messaging services.

9. Follow the installation Configuration Wizard prompts.

   The system upgrades the Modular Messaging software components. The components window shows which component is being installed. The system pauses for several minutes when installing the Avaya SPIRIT Agent. This is normal. Also, this step might take several minutes for a large database or a global address list (GAL).

10. If you installed Web Subscriber Options, follow the prompts to complete the installation wizard.

11. When the Installation Wizard flashes a warning that installation is not complete, restart the system and log back on as the Modular Messaging customer account (such as *mmacct*).

    The Installation Configuration Wizard runs automatically displaying the Service Configuration window.

12. When the update is complete, click **Finish**.

13. Remove the media from the DVD drive.

14. Verify the settings of the MM Services. If any are incorrect, reset them to the correct setting.

15. If you disabled the antivirus software on this MAS, enable it again now.

Completing server setup

- Verifying antivirus software on page 163
- Installing software updates on page 163
- Updating Microsoft Windows on page 164
- Enabling ports on page 164
- Completing the Release 3.x or 4.0 to Release 5.2 upgrade on page 165
- Updating client software on page 254

Verifying antivirus software

Avaya strongly recommends that antivirus software be installed on any Microsoft Windows computer that runs Avaya Modular Messaging software. The type of virus-checking software used and the method of installation depends on customer requirements and the local implementation. Verify that the MAS is running the latest version of the antivirus software. For additional guidelines for configuring antivirus software, see Administering antivirus software on page 54.

Installing software updates

A new Modular Messaging system ships with the most current software that is available at the time. However, the software must be updated after an upgrade to include the latest changes. The updates might be in the form of an Avaya Service Pack (SP) or a software patch (hot fix).

To determine if a Modular Messaging software update is needed:

1. Locate any relevant Avaya software updates on the Avaya Support Web site at http://www.avaya.com/support. For complete steps, see Obtaining software updates from the Web on page 303.

   Note:

   If you followed the procedure for Downloading software updates on page 4, you already downloaded any required software updates.

2. If the Modular Messaging system requires a software update, complete the update procedure now before you do acceptance testing. Follow the instructions in Appendix E: Updating Modular Messaging software on page 303 to update the system with the latest changes.

Updating Microsoft Windows

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

Note:

Avaya technical support representatives must follow their specified internal procedures for verifying the software that is installed. If required, they must update the software with the latest patches as instructed.

Enabling ports

Enable the ports on the MAS that you are upgrading.

Use the port monitor to enable the MAS ports:

1. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Port Monitor**.
2. In the **Port Monitor** window, hold down the **Shift** key or Control (**Ctrl**) key and click to select all the ports.
3. Right-click the port list and select **Enable**.
4. Verify that the status of all ports is **Enabled**.
5. Close the **Port Monitor** window

Completing the Release 3.x or 4.0 to Release 5.2 upgrade

This section describes the topics required to complete the upgrade of Modular Messaging system to Release 5.2.

Continue the Modular Messaging software upgrade as appropriate:

1. Install and configure the WebLM server. Use one of the following methods:
   - To install WebLM server on an MAS or a Supplementary server, proceed with Installing WebLM server on an MAS on page 90.
   - If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
   - To install WebLM server on a standalone server, see *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at http://www.avaya.com/support.
2. If you have more than one MAS:
   a. ***For the first MAS upgraded only,*** let the Modular Messaging software run for 15 minutes. Return to Switching the monitor to show the correct server on page 150 to begin upgrading the next MAS.
   b. Repeat the Modular Messaging software upgrade procedure until all MASs are upgraded.

   CAUTION:

   Perform steps 3 and 4 only if you are upgrading from Modular Messaging Release 3.x to Release 5.2.
3. Enable and configure MM Fax Service. If this MAS is to run the MM Fax Sender Service, complete the following steps:
   a. Navigate to the **C:\Avaya_Support\Utils** directory.
   b. Double-click the **FaxSenderEnable.exe** file.
   c. Restart Microsoft Windows Fax Service.
   d. Configure MM Fax Service by completing the steps described in Configuring the MM Fax Sender server on page 96.

   Note:

   Fax Sender Service running with a QSIG T1 or QSIG E1 integration requires the D480JCT-1T1, D/600JCT-1E1 or D/600JCT-2E1 dual span QSIG board. If run with the D/240JCT-T1 or D/300JCT-1E1 board, you must upgrade your board before the system can run the Fax Sender Service. The dual span QSIG boards also require configuration of the **FirmwareFile 2** parameter on the **Intel Dialogic product Configuration Manager - Properties** window. For more information, see Configuring T1-QSIG or E1-QSIG boards on page 310.

4. Configure Audit service by completing the steps described in Configuring Audit Service on page 96.
5. Configure and activate additional new Release 5.2 features as needed using the Voice Mail System Configuration program.
6. Enable all scheduled tasks that you disabled before starting the upgrade.
7. Update the Modular Messaging Active Directory Exchange extensions on machines where they are installed. See Chapter 3: Adding Exchange extensions for Modular Messaging on page 37.

   Note:

   The Modular Messaging Active Directory Exchange extensions are updated along with other Modular Messaging software that is installed on this machine (multiple Modular Messaging software component check boxes might be selected). This ensures that all currently installed components are upgraded. The components are installed in the correct order when you click **Install**.
8. Update the client software on non-MAS machines where it is installed. See Updating client software on page 254.
9. When finished with each MAS, verify that the MAS disk is in good condition by running the following:
   - Disk Defragmenter system tool
   - **chkdsk** command
10. Do the acceptance tests that are appropriate for each server; see Performing acceptance tests on page 112. For example:
    a. For an MAS, test to check if the server can send and receive calls.
    b. For all servers, verify that the services run on the appropriate server.
11. Run a DCT analyze on the system; see Using the DCT to collect information from an MAS on page 152.
12. Complete the following steps to verify all Personal Operator Schedules:
    a. Click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**.
    b. Under the voice mail domain name, double-click **Telephone User Interface**.
    c. Select the **Personal Operator Schedules** tab.
    d. Verify that all Personal Operator Schedules recorded before the upgrade are included in the list. If a schedule is missing, complete the following steps:
       1. Click the **Add** button
       2. In the **Enter Personal Operator Schedule Name** dialog box in the **Schedule Name** field, enter the name of the missing schedule.
       3. Click **OK** to return to the **Personal Operator Schedules** tab.

4. In the schedule grid, enter the schedule times.

e. Click each Personal Operator Schedule in the schedule list and verify that the schedule times correspond to the times recorded before the upgrade. Correct discrepancies in the schedule grid.

f. Close all windows.

13. Review event and alarm logs and resolve problems; obtain the *Avaya Modular Messaging MAS Administration Guide*; see Downloading user documentation on page 5.

14. Run backups on each MAS; see Backing up the MAS on page 155.

15. Perform this step *only* if you are upgrading from Release 3.x. Due to a change in file names, old logs might remain on the system. Remove old logs from ***c:\avaya_support\logs*** folder on each MAS and delete logs that are older than the upgrade's start time.

16. On the MAS, enable alarms:

    a. Configure the SNMP trap destination and community details using the **Serviceability - Voice Mail Domain** window of the Voice Mail System Configuration program. Enter the SNMP trap destination and community information you recorded before beginning the upgrade.

    b. Click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**.

    c. Under the voice mail domain name, double-click **Serviceability**.

    d. On the **Serviceability** page, on the **General** tab, clear the **Suppress alarm notifications** check box, to turn on the alarm notifications options.

    e. Click **Save** to save the changes.

    f. Close all windows.

17. If you are adding a new MAS to this system, begin the installation now.

For post-install procedure of. the MAS,
see Post-installation procedures for Modular Messaging on page 253.

Chapter 10: Migrating to Modular Messaging Release 5.2 on an Avaya MAS

The chapter describes how to migrate from Modular Messaging Release 3.x, Release 4.0, or Release 5.1 running on an S3400 server, S3500 server, or S8730 server to a Modular Messaging Release 5.2 system that runs on an S8800 1U server.

The migration consists of adding additional servers to the customers network where the newly added servers works along side the existing servers until the old ones are removed. Because, the servers have unique names, it is necessary to update the user clients with the new data.

You can reduce the number of MASs in your VMD when migrating from S3400 servers to S8800 1U servers. If you are going to reduce the number of servers, do so before migrating the remaining servers to Release 5.2. See Reducing the number of servers on page 191 for more information.

Topics in this chapter include:

- Migration requirements on page 169
- Preparing for the migration on page 172
- Changing Switch Integration on page 174
- Analyzing the existing system on page 176
- Verifying and saving data on page 176
- Backing up the MAS on page 177
- Configuring the new S8800 1U server on page 178
- Completing the server setup on page 185
- Disabling the Avaya S3400, S3500, or S8730 servers on page 189
- Completing the migration on page 190
- Reducing the number of servers on page 191

Migration requirements

To successfully migrate a Modular Messaging system:

- You need a replacement server with preloaded Avaya Modular Messaging Application Server (MAS) and boot software.

- Before you migrate the MASs, the domain administrator must create a computer account for the new server. See Creating MAS computer accounts on page 31 for more information.
- Download the *Avaya Modular Messaging Documentation* from the http://www.avaya.com/support.
- All account names and passwords must conform to Windows 2003 security rules. If your account names and passwords do not conform to the new rules, you must change them before you analyze your system with the DCT executable file (**MMDCT.exe**). If you must change your Modular Messaging account names or passwords, contact your support organization for more information.
- Planning forms for the system that runs on Release 3.x or the original DCT file for a system that runs on Release 4.0 or Release 5.1.
- You need Microsoft Exchange Server MAPI Client for a system with Microsoft Exchange 2007 or Exchange 2010 mail servers. Download the MAPI Client from the following site:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=e17e7f31-079a-43a9-bff2-0a110307611e&DisplayLang=en.
- You need PowerShell 2.0 for Exchange 2010 or PowerShell 1.0 or later for Exchange 2007.
- The following information and software from the Avaya Support Web site at http://www.avaya.com/support. For more information about how to access these items on the Web site, see Downloading required software and documentation on page 3.
  - The latest copy of the configuration notes for this switch integration.
  - Any Avaya software updates and third-party software required to bring the Avaya Modular Messaging software up to date after the migration is complete. Download this software to a USB storage device such as a flash drive, memory stick, or equivalent.
  - The latest version of MMDCT.exe.
- Print the migration checklist from Appendix A: Installation, upgrade, and migration checklists on page 225. Use the checklist to track your progress.

18. Install and configure the WebLM server. Use one of the following methods:
    - To install WebLM server on an MAS or a Supplementary server, proceed with Installing WebLM server on an MAS on page 90.
    - If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
    - To install WebLM server on a standalone server, see *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at http://www.avaya.com/support.
- Customer-provided Microsoft Exchange System Management Tools. For more information, see Installing third-party software on page 181.

- For a system with Exchange 2007 mail servers, you will require the 32-bit version of the Exchange 2007 Management Tools, Microsoft Exchange 2007 Service Pack 1, and additional software downloads. You may download the 32-bit version of the Exchange 2007 Management Tools from:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=444C259E-605F-4A82-96D5-A2F448C9D4FF&displaylang=en

- For a system with Exchange 2003 mail servers, you will require Microsoft Exchange Service Pack 2 for Exchange 2003 System Management Tools, and additional software downloads.

Preparing for the migration

This section describes how to prepare the Modular Messaging system that runs on an S3400 server, S3500 server, or an S8730 server to migrate to Modular Messaging Release 5.2 running on an S8800 1U server.

When migrating from an S3400 hardware, you may reduce the number of MASs in your VMD. For complete procedures to reduce MASs, see Reducing the number of servers on page 191.

To migrate the system to Modular Messaging Release 5.2:

1. Review the configuration notes for any changes that might be needed in the areas of board configuration, switch programming, and application configuration. For more information, see Migration requirements on page 169.
2. Change the Switch Integration type to SIP. For more information, see Changing Switch Integration on page 174
3. Use the DCT to analyze the existing servers. For more information, see Analyzing the existing system on page 176. If you are reducing the number of servers, include the servers that are being removed from the VMD.

   Note:

   Also, include the Supplementary server, if present.
4. Verify and save the data on the MAS that is being replaced.
5. Back up the MAS that is being replaced.
6. Add the new S8800 1U MAS to the system using the DCT data file created by the system analysis.
7. Complete setup of the new S8800 1U server by administering antivirus software, installing software updates, updating Windows, changing LAN name and power management settings, and entering RAS IP addresses on the MAS.

- Obtain and activate new PLDS license file on the WebLM server. For more information, see:
  - Installing and configuring the WebLM server on an MAS on page 89
  - Obtaining the license file on page 91
  - Applying license file on the WebLM server on page 91.

8. Disable Modular Messaging services on the server that is being replaced.
9. Move the disabled services to the new S8800 1U server and enable them.
10. Restore customer data to the new S8800 1U server.
11. Configure new Release 5.2 features and verify that required services are running.

12. Update Exchange extensions and client software on client machines where it was previously installed. See detailed steps in Chapter 3: Adding Exchange extensions for Modular Messaging on page 37 and Updating client software on page 254.

    Note:

    Schedule downtime for the Exchange Server if the Modular Messaging Subscriber Administration components need to be upgraded on the Exchange server and if the Exchange server prompts you for a restart.

13. Test and back up the new S8800 1U server. See Completing the migration on page 190.
14. Remove the server that is being replaced from the system.

Considerations for multiple-MAS migration

In a multiple-MAS configuration, Avaya strongly recommends that all MASs be migrated to Modular Messaging Release 5.2 software as soon as possible. During a migration, MASs in the same Voice Mail Domain can run different releases of Modular Messaging. However, at the completion of a migration, all MASs in the Voice Mail Domain must be running Release 5.2.

All MASs in the voice mail domain must be migrated to the same release of Modular Messaging software before you can enable the new Release 5.2 features.

Changing Switch Integration

The switch integrations may use different Dialogic port boards or may not use a Dialogic port board. Use the procedures described in Configuring port boards and switch integration on page 100 and procedures described in Configuring and testing port boards on page 307.

If you are migrating from a S3400, S3500, or S8730 server, you must change the switch integration to SIP. To convert from DSE, QSIG, or H.323 to SIP, see the relevant section below:

- Changing from Analog, DSE, or QSIG to SIP on page 174
- Changing from H.323 to SIP on page 175

Changing from Analog, DSE, or QSIG to SIP

1. Using VMSC, change the Switch Integration type to SIP for the MAS (start with MAS#1) and make all VMSC configuration changes as documented in the SIP Switch Integration Configuration note (for note information, see the Avaya Support Web site at http://www.avaya.com/support).
2. Using VMSC, change the number of ports for the MAS to the number of ports required with your SIP integration.
3. Restart the messaging service and set all services to **Automatic**; see Restarting messaging services on page 102.
4. After the messaging service has restarted and the system has produced the NT Application 1241 event, run the utility **`C:\Avaya_Support\Tools\ConfigureMMIPSEC\ConfigureMMIPSEC.exe`**
5. Test the SIP integration; see Verifying call-handling capability on page 104.
6. Shut down the MAS.
7. Remove the Dialogic boards from the MAS.

   See *Avaya Modular Messaging S8730-Family Hardware Maintenance and Additions* guide, *Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions* guide, or *Avaya Modular Messaging S3400-Family Hardware Maintenance and Additions* guide for information on board removal.
8. Start the MAS without any Dialogic boards installed.
9. Make sure that all MM Services start up properly.
10. Repeat the steps for each MAS you plan to move to the SIP integration.

Changing from H.323 to SIP

For changing the H.323 to SIP, you need to:

1. Using VMSC, change the Switch Integration type to SIP for the MAS (start with MAS#1) and make all VMSC configuration changes as documented in the SIP Switch Integration Configuration note (for note information, see the Avaya Support Web site at http://www.avaya.com/support).
2. Using VMSC, change the number of ports for the MAS to the number of ports required with your SIP integration.
3. Restart the messaging service and set all services to **Automatic**; see Restarting messaging services on page 102.
4. After the messaging service has restarted and the system has produced the NT Application 1241 event, run the utility **`C:\Avaya_Support\Tools\ConfigureMMIPSEC\ConfigureMMIPSEC.exe`**
5. Test the SIP integration; see Verifying call-handling capability on page 104.
6. Repeat the steps for each MAS in the VMD you plan to move to the SIP integration.

Analyzing the existing system

Analyze the existing system by using the Avaya Modular Messaging Data Collection Tool (DCT) to collect information from each MAS and Supplementary server. See Using the DCT to collect information from an MAS on page 130 for more information.

Verifying and saving data

It is important that you record all critical system settings and back up all data in advance. Complete the following tasks before you start a Release 5.2 migration:

1. Verify key settings on the MAS, including:
   - Switch integration settings
   - Port board settings and extensions
   - Domain information
   - Basic system setup
   - Modular Messaging service account and group
   - Exchange settings

   Make sure that you record the following items:
   - Under **Routing and Remote Access**, record the IP addresses for the MAS modems in the remote access service (RAS) group.
   - In the VMSC for each MAS, record any *non-default* port groups and their names, such as the MWI port group.
   - Record which Modular Messaging services are running on each MAS.
   - SAL destination and community details from the **Serviceability — Voice Mail Domain** window.
2. Complete the following steps to record all personal operator schedules. This information will be required to verify the schedules following the upgrade.
   a. Click **Start > Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration**.
   b. Under the voice mail domain name, double-click **Telephone User Interface**.
   c. Select the **Attendant Schedules** tab.

d. Click each schedule listed in the Schedules box and record the times set for each schedule.

e. Close all windows.

3. If you use this MAS to create, administer, and deploy caller applications, back up all your working files to a location other than the MAS. Make a copy of the entire callerapps directory. The entire folder and its structure must be restored.
4. Make a complete backup of all customized tone files, customized prompt files, licensing files, WSO files and SIP certificates for SIP implementations. Also back up the system state and spool. See Backing up the system on page 119 for information about where to locate these files on your system.
5. Check for errors or warnings on the system. Resolve major and minor alarms.
6. Review product functionality with the customer, including:
   - Differences that will be noticeable to the customer
   - Known issues; see Product Support Notices (PSNs) on the Avaya support Web site
   - Rollout plan for new features
   - Security concerns

Backing up the MAS

Before beginning the migration, make a current backup of the important system files on the server that is being replaced, including any customized tone files. Also, back up the DCT data file that you just created. For this procedure, see Backing up the system on page 119.

Configuring the new S8800 1U server

You must add the new S8800 1U server to the system by completing the following steps:

- Adding the new S8800 1U server on page 178
- Installing third-party software on page 181
- Completing the MMCW configuration on page 183

Adding the new S8800 1U server

After the server boots, the Avaya Modular Messaging Configuration wizard runs automatically.

Note:

Before you turn on the server you want to configure, insert the storage device. The server can easily recognize the storage device if the device is already inserted when the server boots.

To configure the new server:

1. On the **Welcome** screen, click **Next**.
2. On the **Locate Configuration Data** screen, click **Browse**.
   a. In the **Open** window, click the drop-down list next to **Look in**.
   b. Navigate to the storage device, **Removable disc (E:)**.

      If the server fails to recognize the storage device, you can:

      1. In the **Open** window, click **My Computer** in the left pane. After the Look in field shows **My Computer**, press **F5** to refresh the screen.
      2. If the storage device still fails to appear, remove and then insert the device again.

   c. Double-click the most current data file on the storage device, such as *sitefile.mmdct*.
3. On the **Locate Configuration Data** screen, click **Next**.
4. When the system prompts you to confirm the data file, click **Yes**.

   The **Avaya Modular Messaging Data Collection Tool** window opens.
5. Update the following screens:
   a. Navigate through the first few screens and verify the data. Click **Next** on each screen.
   b. Under **MM servers**, click **Message store**. On the system **Message store** screen, select server with **Avaya MAS servers**.

c. Under **MM servers**, click **Voice Mail Domain**. On the system **Voice Mail Domain** screen complete the following:

   1. Update the Number of MASs in the VMD by increasing the number of MASs by 1 to include the MAS you are adding.
   2. The system displays a warning that you are changing the number of MAS servers in the Voice Mail Domain. You must analyze the system at the end of this procedure to make sure that the data file reflects the changes you make. Click **OK**.
   3. Click **Next**.

d. Under **Networking**, click **Corporate server networking details**. The system displays **Corporate server networking** details screen.

   - Enter the values in the **Full Computer Name** field and the **IP address** field for the server that you are adding. The values entered should be unique, since it will be in service at the same time as the old server.

e. Under **Accounts and passwords**, click **MAS accounts and passwords**. The system displays MAS accounts and passwords screen.

   - Enter the Local administrator account details in the **Logon name** and the **Password** fields for each MAS and Supplementary server.

f. If the server is to run the Messaging Application Server service and handle calls, then in **TTS sessions and languages**, click **TTS and announcements**. The system displays **TTS and announcements** screen.

   - Select required announcement and TTS languages. Also enter the TTS sessions for each MAS.

g. On the WebLM Server screen, complete the WebLM settings:

   1. Select the server on which you install the WebLM server:
      - On a MAS or supplementary server
      - On an Avaya optional server or customer provided equipment
   2. MAS Number
   3. WebLM Server URL
   4. Click **Next**.

h. In **MAS servers**, click **MM service selection**. The system displays **MM service selection** screen.

CAUTION:

Do not attempt to move services using this screen! Leave all the Modular Messaging services set exactly as they are. Do not move services from one column to another, or you will damage the operation of the system.

- For an MAS, select *only* the **Message Application** check box. Leave all other services set as they are.

- For a supplementary server, *do not* select the **Message Application** check box. Do not select any other services. Leave the **MAS** column for the new server blank.

i. Click **Save**.

6. Save the updated data file to the storage device:
   a. When the system prompts you to save the file, click **Yes**.
   b. In the **Save As** window, navigate to the storage device.
   c. Type the name of the data file in the **File name** field, such as *sitefile*.
   d. Leave the file type set as *.mmdct*.
   e. Click **Save**.
   f. If the system prompts you to replace an existing data file, click **Yes**.
7. To continue the configuration process, click **Complete**.
8. The system prompts you to save the file.

   You *must* ***Save the file*** even if no changes were made.

   The system automatically saves the updated data file to the ***C:\Program Files\Avaya Modular Messaging\Install\MISCM\cfg*** directory on the new server.

   The system returns you to the Avaya Modular Messaging Configuration Wizard.
9. On the **Messaging Application Server Number** screen:
   a. Change the **MAS number** field to show the correct number for this server.
   b. Click **Next**.

   The **Configuring System** screen shows the MAS configuration starting. The **Sysprep** window opens. The server then restarts.
10. After the restart starts, a Windows Setup wizard runs. To complete the wizard:
    a. On the **License Agreement** screen, select **I accept this agreement**. Click **Next**.
    b. On the **Your Product Key** screen, type the Windows product key for this server.
       - Each Windows computer has a unique product key for the Windows 2003 R2 operating system. Enter the number exactly as shown.
       - On an S8800 1U server, the product key sticker is located on top of the server chassis.
    c. Click **Next**.

       The Avaya Modular Messaging Configuration Wizard displays the configuration status. The server restarts several times and automatically logs on. If during this stage of the installation the automatic logon fails, log on manually to the server as the Modular Messaging Customer Account. The Modular Messaging Configuration Wizard pauses at Install Third Party Software dialog.

11. The User Administration Extensions should be installed at this time onto the Messaging Application Server. See Adding the Exchange extensions on page 40.
12. Complete the tasks outlined in Installing third-party software on page 181.

Installing third-party software

To install third party software, perform the following:

- If you are installing third-party software from a mapped network drive, update Windows Internet Explorer 7 security. See Updating Windows Internet Explorer 7 security on page 181.
- For Exchange 2010, see Installing third-party software for Exchange 2010 on page 182
- For Exchange 2007, see Installing third-party software for Exchange 2007 on page 182
- For Exchange 2003, see Installing third-party software for Exchange 2003 on page 183

Updating Windows Internet Explorer 7 security

Note:

When prompted to install third-party software, complete this procedure first if you are installing third-party software from a network drive. If you are installing third-party software from a disc or other removable media, such as a USB memory stick, you can skip this procedure and continue with Installing third-party software on page 181.

Before you install any third-party software, such as antivirus software, you need to update Windows Internet Explorer 7 security. If you do not make this update and you try to use a domain account, such as *custacct*, to install third-party software, Windows does not allow the installation.

1. Launch Windows Internet Explorer 7.
2. A window appears that states Windows Internet Explorer Enhanced Security is enabled; click **OK**.
3. From the browser, select **Tools** > **Internet Options**.
4. From the **Internet Options** window, select the **Security** tab.
5. In the **Select a zone to view or change security settings** box, click **Local intranet**.
6. Click **Sites**.
7. On the **Local intranet** window, click **Advanced**.
8. In the **Add this website to the zone** field, enter any one of the following:
   - *<drive letter>:*\, if you are using a mapped drive,

- \\<*computername*>\<*share*\, if you are using a fully qualified domain name (FQDN) in the uniform naming convention (UNC) path,
- the IP address, if you are specifying IP address in the UNC path.

9. Click **Add**.
10. Click **OK** to close the **Local intranet** window.
11. Click **OK** to close the **Internet Options** window.

Installing third-party software for Exchange 2010

Use the procedures in this section to install third-party software when installing Modular Messaging with an Exchange 2010 peer mail server.

When prompted to install third-party software:

1. Install the MAPI Client (v6.5.8190 or later) by double-clicking the MAPI executable file.
2. Install PowerShell 2.0.
3. If you are using Exchange 2007 and Exchange 2010 in a mixed environment, then install Exchange Management Tools for Exchange 2007.
4. Install antivirus software. For more details, see Administering antivirus software on page 54.
5. Complete the MMCW configuration. For details, see Completing the MMCW configuration on page 183.

Installing third-party software for Exchange 2007

Use the procedures in this section to install third-party software when installing Modular Messaging with an Exchange 2007 peer mail server.

When prompted to install third-party software:

1. Install the MAPI Client by double-clicking the MAPI executable file.
2. Install Microsoft Exchange 2007 Management Tools:
   a. Double-click the tools executable file.
   b. Double-click the extracted Microsoft Exchange Installation wizard.
   c. Complete the Microsoft Exchange Installation Wizard selecting **Custom Exchange Server Installation**. Elect to install the **Management Tools**. For details about this procedure, see the Microsoft Exchange documentation.

   You may be prompted to download and install additional components and hotfixes. Follow the installation prompts. Be sure to download the Windows 2003 32-bit version of each component.
3. If prompted, restart the system.

4. Verify that the Exchange Management Tools can communicate with the Exchange 2007 mail server.
5. Follow site-specific procedures to install Microsoft Exchange Server 2007 Service Pack 1.
6. Install antivirus software.see Administering antivirus software on page 54.
7. After installing third-party software, continue with Completing the MMCW configuration on page 183.

Installing third-party software for Exchange 2003

When prompted to install third-party software:

1. Insert the customer-provided Microsoft Exchange Server media in the MAS drive.
2. Install the Management Tools by completing the Microsoft Exchange Installation Wizard.
3. If you receive a compatibility warning, click **Continue**.
4. For details about this procedure, see the Microsoft Exchange documentation.
5. Install Microsoft Exchange Service Pack 2 and additional software downloads.
6. Installing antivirus software. See Administering antivirus software on page 54.
7. After installing third-party software, continue with Completing the MMCW configuration on page 183.

Completing the MMCW configuration

After third-party software is installed, continue with the following steps to complete the configuration:

1. Verify that the *Avaya Modular Messaging Messaging Application Server Software* media is in the MAS DVD drive. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
2. In the third-party dialog box, click **Continue with installation after installing 3rd-party software** on the 3rd-party dialog box. The MMCW resumes with the following sequence of events:
   - The **Setup** screen displays, followed by the **System Upgrade** screen.
   - The system restarts and logs on without user intervention.
   - MMCW restarts automatically and runs the MM Application Setup, installing all Modular Messaging components.
   - After another restart and auto log on, the MMCW continues the system configuration, displaying informational messages, as each component, such as, remote access is configured.

3. When MAS configuration is complete, the progress bar stretches across the window and the Next button becomes active. Click **Next**.
4. On the **WSO configuration** screen, click **Finish**.
5. To complete setup of the Modular Messaging server, proceed to Completing the server setup on page 185.

Completing the server setup

This section describes how to update and protect the new server. To prepare a new server, follow these procedures:

- Installing and configuring WebLM server on page 185
- Applying license file on the WebLM server on page 91
- Installing software updates on page 185
- Updating Microsoft Windows on page 186
- Disabling the private LAN on page 186
- Entering RAS IP addresses on each MAS on page 186

Installing and configuring WebLM server

Use one of the following methods to install and configure the WebLM server:

- To install WebLM server on an MAS or a Supplementary server, proceed with Installing WebLM server on an MAS on page 90.
- If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
- To install WebLM server on a standalone server, see *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at http://www.avaya.com/support.

Installing software updates

The Modular Messaging Release 5.2 software is the most current version available at the time of release. However, you need to update the software after a migration to include the latest changes. Avaya provides these updates in the form of an Avaya Service Pack (SP) or a software patch.

To determine if a Modular Messaging software update is needed:

1. Locate relevant Avaya software updates on the Avaya Support Web site at http://www.avaya.com/support. For complete steps, see Obtaining software updates from the Web on page 303.

   Note:

   If you followed the procedure for Downloading software updates on page 4, you would have already downloaded any required software updates.

If the Modular Messaging system requires a software update, do the update procedure now, before you do acceptance testing. Use the instructions in Appendix E: Updating Modular Messaging software on page 303 to update the system with the latest changes.

Updating Microsoft Windows

A new Avaya MAS contains the most current Microsoft Windows software at the time it is shipped. After a migration, 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.

Note:

Avaya technical support representatives must follow the specified internal procedures to verify the software that is installed. If required, the support representative must update the software with the latest patches as instructed.

Disabling the private LAN

The Modular Messaging private LAN is not used with Microsoft Exchange configurations. Disable the private LAN by completing the following steps:

1. On the desktop, right-click the **Network Places** icon. Select **Properties**.
2. In the **Network Connections** window, highlight **IBM USB Remote NDIS Network Device**. Right-click your selection. From the drop-down list, select **disable** to disable the device.
3. In the **Network Connections** window, highlight **Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client) #2**. Right-click your selection. From the drop-down list, select **disable** to disable the device.
4. In the **Network Connections** window, from the toolbar menu, select **Advanced** > **Advanced Settings**. Verify that the corporate LAN is listed at the top of the list of connections. If not, highlight the name of the corporate LAN and use the arrows to move it up in the list. When finished, close the **Advanced Settings** and **Network Connections** windows.

Entering RAS IP addresses on each MAS

The Avaya Modular Messaging Configuration Wizard automatically sets up inbound remote access to each MAS modem. You must edit the preprogrammed RAS IP addresses to use the addresses that the technical support organization requires.

CAUTION:

If Avaya is to support this system, you must enter the RAS IP addresses assigned by the Avaya Automatic Registration Tool (ART). Otherwise remote access for Avaya technical support will not work.

Complete the following steps for each MAS to set up the IP addresses on MAS to allow remote access:

1. Double-click the **Configure** icon on the desktop.
2. In the left pane of the **Configure** window, expand **Routing and Remote Access**.
3. Expand the server name.
4. Verify authentication:
   a. Highlight **Remote Access Policies**.
   b. On the right pane, double-click **Connections to Microsoft routing and remote access**.
   c. Click the **Edit Profile..** button.
   d. Select the **Authentication** tab.
   e. Make sure that all check boxes (except for the **Unauthenticated access** check box) are selected. If necessary, clear the **Unauthenticated access** check box.
   f. Click **OK**.
   g. If a dialog box appears, click **No**.
   h. Click **OK**.
5. Right-click the server name from the pop-up menu and select **Properties**.
6. Set up PAP security:
   a. In the **Local Properties** window, click the **Security** tab.
   b. Click **Authentication Methods...**
   c. Select **Unencrypted Password (PAP)**.
   d. Verify that all other check boxes are blank. If necessary, clear the check boxes.
   e. Click **OK**.
7. Set up a static IP address pool as follows:
   a. In the local **Properties** window, click the **IP** tab.
   b. Under **IP address assignment**, select **Static address pool**.
   c. Add or edit the address range as follows:
      - If the window shows an incorrect IP address range, select the displayed range and click **Edit**.

CAUTION:

If Avaya supports this server, do not use the preprogrammed IP addresses. You must Edit and Remove these addresses for remote access to work.

- If no address range is already entered, click **Add**.

d. In the **Address Range** dialog box, enter the correct start and end IP addresses for this server.To get the start and end IP addresses, you *must* register your system.

e. Verify that the number of addresses is **2**.

f. Click **OK**.

g. In the **Adapter** field, select **Allow RAS to select adapter**.

h. Click **OK** to close the **Properties** window.

i. If a dialog box appears, click **No**.

j. Close the **Configure** window.

Disabling the Avaya S3400, S3500, or S8730 servers

You need to disable the S3400 server, S3500 server, or S8730 server that is being replaced.

To disable the servers:

- Busying out ports on page 189
- Logging off all remote logins on page 189
- Disabling services on page 190

Busying out ports

Busy out the ports on the MAS that you are replacing and on the switch.

To busy out the ports:

1. The PBX administrator must use the procedures appropriate for this PBX to busy out the ports. Depending on the switch integration, the administrator might be able to temporarily reroute calls to other MASs. If an MAS is unavailable, callers into the system might hear ring-no answer or a busy signal.
2. Use the port monitor to disable the MAS ports:
   a. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Port Monitor**.
   b. In the **Port Monitor** window, hold down the **Shift** key or Control (**Ctrl**) key and click to select all the ports.
   c. Right-click the port list and select **Disable**.
   d. Verify that the status of all ports is **Disabled**.
3. Click **OK** to close this window.

Logging off all remote logins

To log off all remote logins:

1. Log on to the MAS using an account that has administrative permissions.
2. Click **Start** > **Programs** > **Administration**.
3. Open your **Windows Task Manager** and select the **Users** tab.
4. Select remote logins and click **Logoff**.
5. If there are no remote logins, click **Cancel** to exit.

Disabling services

You need to disable the services on the servers you are removing from the existing system. See Disabling Modular Messaging services you plan to move on page 255 for more information.

Completing the migration

To complete the migration of the server you need to:

- Move the services from the server that is being replaced to the new Avaya S8800 1U family-server. See Moving Modular Messaging services among servers on page 257 for more information.
- Restore the customer data, see Restoring the Avaya MAS on page 332.

  Note:

  However, you need not restore the caller apps as it is already restored during the installation of the new Modular Messaging system on the VMD.

  For more information, refer to the *Avaya Modular Messaging Documentation* library.
- Test the Modular Messaging system. For more information, see Chapter 7: Testing and backing up the system on page 107.

  CAUTION:

  Continue with the next step only if the new system has been completely tested and signed off by the customer.
- Remove the S3400, S3500, or S8730 server that you are replacing from the VMD. To remove the servers:

  1. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration** to open the **VMSC window**.
  2. In the **VMSC** window, double-click **Message Application Servers**.
  3. Right-click the name of the server you are removing. Click **Remove**.
- Remove the Modular Messaging components from the server. For more information, see Appendix H: Removing Modular Messaging components from an MAS on page 327.
- Power off the server you are removing.
- You need to repeat the procedure from Verifying and saving data on page 176 for each MAS you need to migrate.

Reducing the number of servers

S8800 1U supports *only* SIP based switch integration and does not support Dialogic port boards.

This migration scenario is only an example that describes how to reduce the number of MASs in your VMD by replacing S3400 servers with S8730 servers.

The Modular Messaging system in the example has four S3400 servers, each running 23 ports of T1 QSIG. Since S8730 server has more port capacity, you need only two S8730 servers, each running 46 ports of T1 QSIG.

Note:

Ensure that the current system is in a like-for-like state prior to the upgrade in terms of the number of MASs, boards, and port configurations or the upgrade fails. Which means you must consolidate and configure the T1 QSIG port boards into two MASs for the current S3400 servers.

1. Move and configure the T1 QSIG port boards:
   a. Move the T1 QSIG board from S3400 MAS#3 to S3400 MAS#1.
   b. Configure the boards using DCM; see Configuring port boards on page 309.
   c. Double-click the **Monitor** icon on the DCM.
   d. Click **Services (Local)** in the left pane, if the item is not already selected.
   e. In the right pane, scroll down to **MM Messaging Application Server**.
   f. Right-click **MM Messaging Application Server** and select **Start**.
   g. Using VMSC, increase the number of ports in S3400 MAS#1 to 46 and allocate the ports to the required port groups.
   h. Restart the Message Application service on the S3400 MAS#1.
   i. Repeat this process to move the T1 QSIG board from S3400 MAS#4 to S3400 MAS#2.
   j. Confirm that all of the ports in each server are working properly before continuing.
   k. Convert the port boards to SIP as outlined in Changing from Analog, DSE, or QSIG to SIP on page 174.
2. Remove MAS#3 and MAS#4 from the VMD:
   a. Log on to MAS#3 as **mmacct**.
   b. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration** to open the **VMSC** window.
   c. In the **VMSC** window, double-click **Message Application Servers**.
   d. Right-click MAS#3 and from the pop-up menu, click **Remove**.
   e. Repeat this process for MAS#4.

f. Shutdown the MAS#3 and MAS#4 S3400 servers.

CAUTION:

Do not use the DCT to move services from one MAS to another during the migration! Moving services might require changes elsewhere in the system, such as on the message store and in the VMSC. Move Modular Messaging services only after the migration is complete.

3. Continue with the migration to Release 5.2; see Analyzing the existing system on page 176.

Chapter 11: Migrating to Modular Messaging Release 5.2 on a customer-provided server

The chapter describes how to migrate from Release 3.x, Release 4.0 or Release 5.1 to a Modular Messaging Release 5.2 system that runs on a customer-provided server.

The migration consists of adding additional servers to the customers network where the newly added servers works along side the existing servers until the old ones are removed. Because, the servers have unique names, it is necessary to update the user clients with the new data.

Topics in this chapter include:

- Migration requirements on page 194
- Preparing for the migration on page 195
- Preparing the customer-provided server on page 197
- Installing and enabling Microsoft Windows services on page 197
- Setting up the new server for Modular Messaging on page 201
- Adding Modular Messaging accounts to the local Administrators group on page 204
- Changing Switch Integration on page 205
- Analyzing the existing system on page 206
- Verifying and saving data on page 206
- Backing up the MAS on page 207
- Installing and Running the Modular Messaging Configuration wizard on page 208
- Completing the server setup on page 216
- Disabling the customer-provided server on page 221
- Completing the migration on page 223

Migration requirements

To successfully migrate a Modular Messaging system, you need:

- Download the *Avaya Modular Messaging Documentation* from the http://www.avaya.com/support.
- All account names and passwords must conform to Windows 2003 security rules. If your account names and passwords do not conform to the new rules, you must change them before you analyze your system with the DCT executable file (**MMDCT.exe**). If you must change your Modular Messaging account names or passwords, contact your support organization for more information.
- Planning forms for the system that runs Release 3.x or original DCT file for the system that runs Release 4.0 or Release 5.1.
- You need Microsoft Exchange Server MAPI Client for a system with Microsoft Exchange 2007 or Exchange 2010 mail servers. Download the MAPI Client from the following site:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=e17e7f31-079a-43a9-bff2-0a110307611e&DisplayLang=en.
- You need PowerShell 2.0 for Exchange 2010 or PowerShell 1.0 or later for Exchange 2007.
- The following information and software from the Avaya Support Web site at http://www.avaya.com/support. For more information about how to access these items on the Web site, see Downloading required software and documentation on page 3.
  - The latest copy of the configuration notes for this switch integration.
  - Any Avaya software updates and third-party software required to bring the Avaya Modular Messaging software up to date after the migration is complete. Download this software to a USB storage device such as a flash drive, memory stick, or equivalent.
  - The latest version of **MMDCT.exe**.
- Print the migration checklist from Appendix A: Installation, upgrade, and migration checklists on page 225. Use the checklist to track your progress.
- New PLDS license file obtained and applied on the WebLM server. Use one of the following methods:
  - To install WebLM server on an MAS or a Supplementary server, proceed with Installing WebLM server on an MAS on page 90.
  - If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
  - To install WebLM server on a standalone server, see *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at http://www.avaya.com/support.

- For more information, see:
  - Installing and configuring the WebLM server on an MAS on page 89.
  - Obtaining the license file on page 91.
  - Applying license file on the WebLM server on page 91.
- Customer-provided Microsoft Exchange System Management Tools from customer Exchange administrator. For more information, see Installing third-party software on page 212.
  - For a system with Exchange 2007 mail servers, you will require the 32-bit version of the Exchange 2007 Management Tools, Microsoft Exchange 2007 Service Pack 1, and additional software downloads. You may download the 32-bit version of the Exchange 2007 Management Tools from:

    http://www.microsoft.com/downloads/details.aspx?FamilyID=444C259E-605F-4A82-96D5-A2F448C9D4FF&displaylang=en
  - For a system with Exchange 2003 mail servers, you will require Microsoft Exchange Service Pack 2 for Exchange 2003 System Management Tools.

Preparing for the migration

This section describes how to add a new Customer-provided server to replace an existing server to run Modular Messaging Release 5.2.

To migrate the system to Modular Messaging Release 5.2:

1. Review the configuration notes for any changes that might be needed in the areas of board configuration, switch programming, and application configuration. For more information, see Migration requirements on page 194.
2. Configure the new Customer-provided server by installing the Microsoft Windows 2003 R2 operating system, setting a computer name, installing Microsoft Windows 2003 SP2, configuring the network card, running recommended disk checks, disabling hyper-threading for IP H.323, joining the Windows domain, adjusting system values, adding Modular Messaging accounts to the local Administrators group and installing Microsoft Windows services.
3. Change the Switch Integration type to SIP. For more information, see Changing Switch Integration on page 205.
4. Use the DCT to analyze the existing servers as well as the servers. For more information, see Analyzing the existing system on page 206.

   Note:

   Also, include the Supplementary server, if present.

5. Verify and save the data on the MAS that is being replaced.
6. Back up the MAS that is being replaced.
7. Add the new customer-provided MAS to the system using the DCT data file created by the system analysis.
8. Complete setup of the new customer-provided sever by administering antivirus software, installing software updates, updating Windows, verifying power management settings, entering RAS IP addresses on the MAS, and setting the logging location.
9. Install WebLM server and apply license file.
10. Disable Modular Messaging services on the server that is being replaced.
11. Move the disabled services to the new customer-provided server and enable them.
12. Restore customer data to the new customer-provided server.
13. Configure new Release 5.2 features and verify that required services are running.
14. Update Exchange extensions and client software on client machines where it was previously installed. See detailed steps in Chapter 3: Adding Exchange extensions for Modular Messaging on page 37 and Updating client software on page 254.

    Note:

    Schedule downtime for the Exchange Server if the Modular Messaging Subscriber Administration components need to be upgraded on the Exchange server and if the Exchange server prompts you for a restart.
15. Test and back up the new server. See Completing the migration on page 223.
16. Remove the server that is being replaced from the system.

Considerations for multiple-MAS migration

In a multiple-MAS configuration, Avaya strongly recommends that all MASs be migrated to Modular Messaging Release 5.2 software as soon as possible. During a migration, MASs in the same Voice Mail Domain can run different releases of Modular Messaging. However, at the completion of a migration, all MASs in the Voice Mail Domain must be running Release 5.2.

All MASs in the voice mail domain must be migrated to the same release of Modular Messaging software before you can enable the new Release 5.2 features.

Preparing the customer-provided server

Complete the following procedures to set up the new customer-provided server to replace the existing server to support Avaya Modular Messaging services.

- Installing Microsoft Windows 2003 R2 operating system on page 197
- Installing and enabling Microsoft Windows services on page 197
- Setting a computer name on page 199
- Installing Microsoft Windows 2003 SP2 on page 199
- Configuring the network card on page 200
- Running recommended disk checks on page 200
- Installing modem drivers on the customer-provided MAS on page 200

Installing Microsoft Windows 2003 R2 operating system

Avaya recommends that you complete a new installation of Windows 2003 R2, when you perform new installations of Modular Messaging with CPE hardware. While installing Windows 2003 R2, make sure that you *only* install the Windows services listed in Installing and enabling Microsoft Windows services on page 197.

Installing and enabling Microsoft Windows services

You must install and enable the Microsoft Windows services on each customer-provided MAS that handles voice calls as described in this section.

To install and enable all required Windows services:

1. Log on to an account that has permissions to install software on this computer, such as the local administrator account.
2. Remove any external hard drives from the MAS.
3. Insert the Microsoft Windows Operating System CD in the MAS drive.
4. Click **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.
5. In the **Add or Remove Programs** window, in the left column, click **Add/Remove Windows Components**.
6. To install Microsoft Windows services:
   a. In the **Windows Components Wizard** window, highlight **Application Server**. Click **Details**.

b. Verify that the following items are checked:
   - Application Server Console
   - ASP.NET
   - Enable COM+ access
   - Message Queuing

   The **Internet Information Services (IIS)** checkbox becomes checked.

c. Highlight **Internet Information Services (IIS)**. Click **Details**. Verify that the following items are checked:
   - Common Files
   - Internet Information Services Manager
   - World Wide Web Server

Note:

When you check these items, IIS gets checked automatically.

The Internet Information Services items listed above are always required.

If you plan to install the Microsoft Exchange 2003 System Management Tools, click the checkboxes for **NNTP Service** and **SMTP Service**. The SMTP Service automatically selects other required components as needed.

If you plan to install the Microsoft Exchange 2007 Management Tools, do *not* install NNTP Service and SMTP Service.

d. In the same window, highlight **World Wide Web Server** and click **Details**. Verify that World Wide Web Services is checked.

e. Close this and the next two windows.

7. Install the Windows services to support SNMP:
   a. in the **Windows Components Wizard** window, highlight **Management and Monitoring Tools** and click **Details**.
   b. Click the check box to select **Simple Network Management Protocol** and click **OK**.
8. Install the Windows Fax Service, in the **Windows Components Wizard** window:
   a. Check **Fax Services**. Click **Next**.
   b. Select **Do Not Share Fax Printer** and click **Next**.
9. Complete the wizard to install the selected services.

Note:

If the required services were already installed (all the appropriate boxes were checked), click **Cancel** to close the wizard.

10. When the installation is complete, close the **Add or Remove Programs** window.
11. After the software is installed, enable each installed service as follows:
    a. Right-click **My Computer** and select **Manage**.
    b. In the left (Tree) pane, expand **Services and Applications**, and click **Services**.
    c. In the right pane, scroll down to the first new service that you installed. Double-click the service.
    d. In the **Properties** window:
        1. On the **General** tab, set the **Startup type** to **Automatic**. Click **Apply**.
        2. Under **Service status**, click **Start**.
        3. Wait for service to start, and then click **OK** to close this window.
    e. Repeat Steps c and d to enable each of the services you installed. Note that only a subset of these services might be present on a particular MAS.
12. When all services are enabled, close all open windows.

Setting a computer name

When installing Windows 2003 R2 on the server, you must manually provide the name of the computer before you run the Modular Messaging Configuration wizard.

Make sure that the name and IP address of the new Customer-provided server being added to the VMD does not conflict with the name and IP address of the existing server that is to be replaced.

Installing Microsoft Windows 2003 SP2

To install Microsoft Windows SP2:

1. Install Microsoft Windows Service Pack 2 on this MAS. Check with the Windows administrator for the appropriate software update procedures to use at this site.
2. Verify the Microsoft Windows service pack version that is installed:
    a. Right-click **My Computer** and select **Properties**.
    b. Verify that Service Pack 2 is installed from the version description under the **System** section of the **General** tab.
    c. Click **OK**.

Configuring the network card

For each customer-provided server, you must configure a network card to support a corporate LAN connection.

Assign IP addresses and other TCP/IP properties for the corporate LAN interface that this MAS will use. The IP address assigned should be different from the existing IP addresses.

Running recommended disk checks

Avaya recommends that the hard disk drive in the server be maintained to prevent possible problems. The system administrator must run the following on a regular basis:

- Disk Defragmenter system tool
- **chkdsk** command

If this server is in service and has not been recently maintained, run the two recommended procedures.

Installing modem drivers on the customer-provided MAS

For customer-provided MAS, the customer must install the drivers for serial adapters, serial port and the modem. Avaya does not take the responsibility of installing modems on the customer-provided MAS.

Setting up the new server for Modular Messaging

You must set up the customer-provided server to support Modular Messaging software as described in this section.

- Joining the Windows domain on page 201
- Adjusting system values on page 202

Joining the Windows domain

You must manually add this server to the appropriate Microsoft Windows domain for this Modular Messaging system:

1. Switch the monitor to show this server.

   Use whatever method is required at this site to have the monitor display the MAS that you are administering.

2. Log on to the local administrator account for this server:

   a. In the **Log On to Windows** window, change the user name to the local administrator account name, such as *mas1-admin*.

   b. Enter the password for this account.

   c. If the **Log in to:** field shows a different domain, use the drop-down box to select this server.

   d. Press **Enter** or click **OK**.

3. Right-click **My Computer** and select **Properties**.

4. In the **System Properties** window:

   a. Click the **Computer Name** tab.

   b. Click **Change**.

5. In the **Computer Name Changes** window:

   a. Under **Member of**, select **Domain**.

   b. Type the name for the corporate Windows domain.

   Note:

   Depending on the local configuration, you might need to enter the fully qualified name here.

   c. Click **OK**.

   d. Another **Computer Name Changes** window might open. If it does:

1. Enter the name of an account that has permissions to join the Windows domain. You usually use the Modular Messaging customer account, if the domain administrator has set up the customer account as described in Creating Modular Messaging customer and technical support accounts on page 10. The account name must be in the format ***domain\account name***, such as *domain1\mmacct*.
2. Enter the password for this account. Click **OK**.

6. If a **Welcome to the domain** message is displayed, click **OK**.
7. When prompted to restart, click **OK**.
8. Click **OK** to close the window.
9. If you are prompted to restart the server, click **Yes**.

Adjusting system values

You must adjust some default values on the server to support Modular Messaging. Verify the following settings, and adjust them if needed:

1. Adjust the values for the Event Viewer:
   a. Right-click **My Computer** and select **Manage**.
   b. In the left pane, expand **Event Viewer**.
   c. Adjust the application log values:
      1. Right-click **Application** and select **Properties**.
      2. On the **General** tab, under **Log size**, adjust the following values:
         - Avaya recommends that you set **Maximum log size** to at least 102400 KB.
         - Select **Overwrite events as needed**.
      3. Click **OK**.
   d. Adjust the system log values:
      1. In the right pane, right-click **System** and select **Properties**.
      2. On the **General** tab, under **Log size**, adjust the following values:
         - Set **Maximum log size** to at least 4032 KB.
         - Select **Overwrite events as needed**.
      3. Click **OK**.
   e. Close the next window.
2. Right-click **Start** and select **Explore**. Adjust File and Printer Sharing properties:
   a. Right-click **My Network Places** and click **Properties**.

b. Right-click **Local Area Connection** and click **Properties**.

c. Select **File and Printer Sharing for Microsoft Networks** and click **Properties**.

d. On the **Server Optimization** tab, select **Maximize data throughput for network applications**.

e. Click **OK**.

f. Close the next two windows.

3. Adjust the Windows Server 2003 operating system values:

a. Right-click **My Computer** and select **Properties**.

b. Click the **Advanced** tab.

c. Under **Performance**, click **Settings**.

d. Click the **Advanced** tab.

1. Under **Processor Scheduling**, select **Background services**.
2. Under **Virtual memory**, click **Change**.
3. The **Initial size** and **Maximum size** fields for the **Paging file size for selected drive** value vary by machine. Tailor these fields by adding 11 to the default value that is displayed as follows:
   - Under **Paging file size for selected drive**, set both the **Initial size** and **Maximum size** to the default value plus 11 MB.
   - Click **Set**.
   - Click **OK**.
4. Close the next window.

e. On the **Advanced** tab:

1. Under **Startup and Recovery**, click **Settings**.
2. In the **Startup and Recovery** window, under **System Failure**, verify that the **Automatically restart** checkbox is checked.
3. Click **OK**.

f. Close the next window.

4. Restart the server before continuing:

- If you are prompted to restart the server, click **Yes**.
- If the system does not prompt you, manually restart the server now. For example:

a. Press **Ctrl**+**Alt**+**Del**. Click **Shut Down**.

b. Select **Restart** from the drop-down list. Click **OK**.

The server restarts.

Adding Modular Messaging accounts to the local Administrators group

For the accounts to work correctly, you must add the Modular Messaging service permissions and the technical support account to the local administrators group:

1. Log on to the local administrator account for this server. For details, see Joining the Windows domain on page 201.
2. Click **Start** > **Control Panel**.
3. Double-click **Administrative Tools**.
4. Double-click **Computer Management**.
5. Under **System Tools**, expand **Local Users and Groups** and then click **Groups**.
6. In the right pane, double-click the **Administrators** group.
7. Click **Add**.
8. In the **Enter object names to select** pane, enter the names of the service permissions and technical support remote access account. The account names must be in the format ***domain\account name*** (such as *domain1\mmacct*).

   Note:

   You can search for the accounts by entering a portion of the name in the **Enter the object names to select** pane, and clicking **Check Names**.

   After names are entered, click **OK**.
9. Close all open windows.

Changing Switch Integration

The switch integrations may use different Dialogic port boards or may not use a Dialogic port board. Use the procedures described in Configuring port boards and switch integration on page 100 and procedures described in Configuring and testing port boards on page 307.

If you are migrating from a S3400, S3500, or S8730 server, you must change the switch integration to SIP. To convert from DSE, QSIG, or H.323 to SIP, see the relevant section below:

- Changing from Analog, DSE, or QSIG to SIP on page 205
- Changing from H.323 to SIP on page 206

Changing from Analog, DSE, or QSIG to SIP

1. Using VMSC, change the Switch Integration type to SIP for the MAS (start with MAS#1) and make all VMSC configuration changes as documented in the SIP Switch Integration Configuration note (for note information, see the Avaya Support Web site at http://www.avaya.com/support).
2. Using VMSC, change the number of ports for the MAS to the number of ports required with your SIP integration.
3. Restart the messaging service and set all services to **Automatic**; see Restarting messaging services on page 102.
4. After the messaging service has restarted and the system has produced the NT Application 1241 event, run the utility **`C:\Avaya_Support\Tools\ConfigureMMIPSEC\ConfigureMMIPSEC.exe`**
5. Test the SIP integration; see Verifying call-handling capability on page 104.
6. Shut down the MAS.
7. Remove the Dialogic boards from the MAS.

   See *Avaya Modular Messaging S8730-Family Hardware Maintenance and Additions* guide, *Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions* guide, or *Avaya Modular Messaging S3400-Family Hardware Maintenance and Additions* guide for information on board removal.
8. Start the MAS without any Dialogic boards installed.
9. Make sure that all MM Services start up properly.
10. Repeat the steps for each MAS you plan to move to the SIP integration.

Changing from H.323 to SIP

For changing the H.323 to SIP, you need to:

1. Using VMSC, change the Switch Integration type to SIP for the MAS (start with MAS#1) and make all VMSC configuration changes as documented in the SIP Switch Integration Configuration note (for note information, see the Avaya Support Web site at http://www.avaya.com/support).
2. Using VMSC, change the number of ports for the MAS to the number of ports required with your SIP integration.
3. Restart the messaging service and set all services to **Automatic**; see Restarting messaging services on page 102.
4. After the messaging service has restarted and the system has produced the NT Application 1241 event, run the utility **`C:\Avaya_Support\Tools\ConfigureMMIPSEC\ConfigureMMIPSEC.exe`**
5. Test the SIP integration; see Verifying call-handling capability on page 104.
6. Repeat the steps for each MAS in the VMD you plan to move to the SIP integration.

Analyzing the existing system

Analyze the existing system by using the Avaya Modular Messaging Data Collection Tool (DCT) to collect information from each MAS and Supplementary server.
See Using the DCT to collect information from an MAS on page 152 for more information.

Verifying and saving data

It is important that you record all critical system settings and back up all data in advance.

Complete the following tasks before you start a Release 5.2 migration.

1. Verify key settings on the MAS, including:
   - Switch integration settings
   - Port board settings and extensions
   - Domain information
   - Basic system setup

- Modular Messaging service account

Ensure that you record the following items:

- Record the IP addresses for the MAS modems in the remote access service (RAS) group.
- In the VMSC for each MAS, record any *non-default* port groups and their names, such as the MWI port group.
- Record which Modular Messaging services are running on each MAS.
- Record the SAL destination and community details from the **Serviceability - Voice Mail Domain** window

2. If the site has caller applications, make sure that a copy of all editable files is on a separate computer, *not* the MAS. See Backing up the system on page 119 for information about where to locate these files on your system.
3. Check for errors or warnings on the system. Resolve major and minor alarms.
4. Review product functionality with the customer, including:
    - Differences that will be noticeable to the customer
    - Known issues; see Product Support Notices (PSNs) on the Avaya support website
    - Rollout plan for new features
    - Security concerns

Backing up the MAS

Before beginning the migration, make a current backup of the important system files, including any customized tone files and the DCT data file that you just created. For this procedure, see Backing up the system on page 119.

Installing and Running the Modular Messaging Configuration wizard

The **Modular Messaging Configuration** wizard controls the next steps in adding the new server to the system. In installing and running the wizard you must complete the following procedures:

- Running the Modular Messaging Configuration wizard on page 208
- Installing third-party software on page 212
- Completing the MMCW configuration on page 214

Installation procedures for Dialogic drivers and the RealSpeak engine differ if you have chosen to install modular messaging to a drive other than the default **C:** drive. Differences are described in each procedure. The drive location for the Modular Messaging installation is set in the DCT data file.

Running the Modular Messaging Configuration wizard

Use the following steps to collect data from each MAS and the supplementary server, if present:

The Modular Messaging Configuration wizard (MMCW) uses the DCT data file to configure the customer-provided MAS. You must install the Modular Messaging Configuration wizard (MMCW) to configure each customer-provided MAS.

Complete the following steps:

1. Verify that the USB storage device with the DCT data file (**.mmdct*) and most recent DCT executable file (**MMDCT.exe**) is inserted in the USB port.
2. Turn the server on.
3. Log on to the MAS using the Modular Messaging customer account created in Creating Modular Messaging customer and technical support accounts on page 10.
4. Insert the ’Avaya Modular Messaging R5.2 MAS Application DVD 1 of 2 disk into the DVD drive of the customer-provided MAS. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
5. Navigate to the ***Install\MISCM*** directory and double-click the ***MMConfigurationWizard.msi*** file.

   The system installs the configuration wizard in the ***C:\Program Files\Avaya Modular Messaging\Install\MISCM*** directory and launches the Modular Messaging configuration wizard.

   Note:

   You need to select the check box on the **Close** screen to launch the MMCW.

6. Click **Finish**.
7. Copy the ***MMDCT.exe*** file from your storage device to ***C:\Program Files\Avaya Modular Messaging\Install\MISCM*** directory.
8. On the **Modular Messaging Welcome** screen, click **Next**.
9. On the **Locate Configuration Data** screen, click **Browse**.
   a. In the **Open** window, click the drop-down list next to **Look in**.
   b. Navigate to the storage device.

      If the server fails to recognize the storage device, you can:

      1. In the Open window, click **My Computer** in the left pane. After the **Look in** field shows **My Computer**, press **F5** to refresh the screen.
      2. If the system fails to display the storage device, unplug the device and insert the device again.

   c. Double-click the most current DCT data file.
10. On the **Locate Configuration Data** screen, click **Next**.
11. When the system prompts you to confirm the data file, click **Yes**.

    The system opens **Avaya Modular Messaging Data Collection Tool** window.
12. Update the following screens:
    a. Navigate through the first few screens and verify the data. Click **Next** on each screen.
    b. Under **MM servers**, click **Message store**. On the system **Message store** screen, if not already selected, select **Microsoft Exchange with customer's MAS servers**.
    c. Under **MM servers**, click **Voice Mail Domain**. On the system **Voice Mail Domain** screen complete the following:

       1. Update the Number of MASs in the VMD by increasing the number of MASs by 1 to include the MAS you are adding.
       2. The system displays a warning that you are changing the number of MAS servers in the Voice Mail Domain. You must analyze the system at the end of this procedure to make sure that the data file reflects the changes you make. Click **OK**.
       3. Click **Next**.

    d. Under **Networking**, click **Corporate server networking details**. The system displays **Corporate server networking** details screen.

       - Enter the values in the **Full Computer Name** field and the **IP address** field for the server that you are adding. The values entered should be unique, since it will be in service at the same time as the old server.

    e. Under **Accounts and passwords**, click **MAS accounts and passwords**. The system displays MAS accounts and passwords screen.

- Enter the Local administrator account details in the **Logon name** and the **Password** fields for each MAS and Supplementary server.

f. If the server is to run the Messaging Application Server service and handle calls, then in **TTS sessions and languages**, click **TTS and announcements**. The system displays **TTS and announcements** screen.

- Select required announcement and TTS languages. Also enter the TTS sessions for each MAS.

g. On the WebLM Server screen, complete the WebLM settings:

1. Select the server on which you install the WebLM server:
   - On a MAS or supplementary server
   - On an Avaya optional server or customer provided equipment
2. MAS Number
3. WebLM Server URL
4. Click **Next**.

h. In **MAS servers**, click **MM service selection**. The system displays **MM service selection** screen.

CAUTION:

Do not attempt to move services using this screen! Leave all the Modular Messaging services set exactly as they are. Do not move services from one column to another, or you will damage the operation of the system.

- For an MAS, select *only* the **Message Application** check box. Leave all other services set as they are.
- For a supplementary server, *do not* select the **Message Application** check box. Do not select any other services. Leave the **MAS** column for the new server blank.

i. Click **Save**.

13. Save the updated data file to the storage device:

a. When the system prompts you to save the file, click **Yes**.

b. In the **Save As** window, navigate to the storage device.

c. Type the name of the data file in the **File name** field, such as *sitefile*.

d. Leave the file type set as *.mmdct*.

e. Click **Save**.

f. If the system prompts you to replace an existing data file, click **Yes**.

14. To continue the configuration process, click **Complete**.

The system automatically saves the updated data file to the ***C:\Program Files\Avaya Modular Messaging\Install\MISCM\cfg*** directory on the new server.

CAUTION:

Make sure you save the DCT file back to the storage device, irrespective of whether you updated any information in the DCT data file or not. You need a current copy for technical support and for subsequent server migrations.

The system returns you to the **Avaya Modular Messaging Configuration Wizard**.

15. On the **Messaging Application Server Number** screen, specify the **MAS number** field to show the correct number for this server.
16. Click **Next**.
17. When the system prompts you to log on, log on to the customer-provided MAS using the administrator account.
18. When the configuration wizard prompts you to locate the ***InstallRSEngine.bat*** file, insert the 'Modular Messaging R5.2 MAS Application DVD 2 of 2' disk. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
19. When you receive the error message that the **<drive>:\Realspeak** location is not available:
    a. Click **OK** to close the dialog box.
    b. In the **Look In** field, choose the DVD drive and double-click the **Realspeak** directory.
    c. Click **Open**.

    The **RealSpeak 4.0 InstallShield** wizard starts.
20. If you are installing Modular Messaging to the default **C:** drive, complete the wizard by accepting all default values. If you are installing Modular Messaging to an alternate drive, complete the following steps:
    a. Move through the RealSpeak installation wizard accepting defaults until you see the **Custom Setup** screen.
    b. On the **Custom Setup** screen, highlight RealSpeak Common Components. Click the arrow next to **RealSpeak Common Components** and select **This feature and all subfeatures will be installed on local hard drive**. Click **Change**.
    c. On the **Change Current Destination Folder** screen, in the **Folder name:** field change the letter of the drive to match the drive where Modular Messaging is being installed. This drive is set in the DCT data file. Do not browse to find the new location. The path will read **<*drive letter*>:\Program Files\ScanSoft\RealSpeak 4.0**.
    d. Click **OK** and continue to accept default values to complete the wizard.
21. After the RealSpeak engine is installed, at the prompt to restart the system, choose to restart.
22. After the system restarts, log on using the customer account, for example *mmacct*. The RealSpeak languages install.
23. Click **Next**.

    The Modular Messaging Configuration wizard pauses at Install Third Party Software dialog.

24. The User Administration Extensions should be installed at this time onto the Messaging Application Server. See Adding the Exchange extensions on page 40.
25. Complete the tasks outlined in Installing third-party software on page 212.

Installing third-party software

Do *not* press **Continue with installation** until you do the following:

- If you are installing third-party software from a mapped network drive, update Windows Internet Explorer 7 security. See Updating Windows Internet Explorer 7 security on page 212.
- For Exchange 2010, see Installing third-party software for Exchange 2010 on page 213
- For Exchange 2007, see Installing third-party software for Exchange 2007 on page 213
- For Exchange 2003, see Installing third-party software for Exchange 2003 on page 214

Updating Windows Internet Explorer 7 security

Note:

When prompted to install third-party software, complete this procedure first if you are installing third-party software from a network drive. If you are installing third-party software from a disc or other removable media, such as a USB memory stick, you can skip this procedure and continue with Installing third-party software on page 212.

Before you install any third-party software, such as antivirus software, you need to update Windows Internet Explorer 7 security. If you do not make this update and you try to use a domain account, such as *custacct*, to install third-party software, Windows does not allow the installation.

1. Launch Windows Internet Explorer 7.
2. A window appears that states Windows Internet Explorer Enhanced Security is enabled; click **OK**.
3. From the browser, select **Tools** > **Internet Options**.
4. From the **Internet Options** window, select the **Security** tab.
5. In the **Select a zone to view or change security settings** box, click **Local intranet**.
6. Click **Sites**.
7. On the **Local intranet** window, click **Advanced**.
8. In the **Add this website to the zone** field, enter any one of the following:
   - <*drive letter*>:\, if you are using a mapped drive,

- \\<*computername*>\<*share*\, if you are using a fully qualified domain name (FQDN) in the uniform naming convention (UNC) path,
- the IP address, if you are specifying IP address in the UNC path.

9. Click **Add**.
10. Click **OK** to close the **Local intranet** window.
11. Click **OK** to close the **Internet Options** window.

Installing third-party software for Exchange 2010

Use the procedures in this section to install third-party software when installing Modular Messaging with an Exchange 2010 peer mail server.

When prompted to install third-party software:

1. Install the MAPI Client (v6.5.8190 or later) by double-clicking the MAPI executable file.
2. Install PowerShell 2.0.
3. If you are using Exchange 2007 and Exchange 2010 in a mixed environment, then install Exchange Management Tools for Exchange 2007.
4. Install antivirus software. For more details, see Administering antivirus software on page 54.
5. Complete the MMCW configuration. For details, see Completing the MMCW configuration on page 214.

Installing third-party software for Exchange 2007

Use the procedures in this section to install third-party software when installing Modular Messaging with an Exchange 2007 peer mail server.

When prompted to install third-party software:

1. Install the MAPI Client by double-clicking the MAPI executable file.
2. Install Microsoft Exchange 2007 Management Tools:
   a. Double-click the tools executable file.
   b. Double-click the extracted Microsoft Exchange Installation wizard.
   c. Complete the Microsoft Exchange Installation wizard selecting **Custom Exchange Server Installation**. Elect to install the **Management Tools**. For details about this procedure, see the Microsoft Exchange documentation.

   You may be prompted to download and install additional components and hotfixes. Follow the installation prompts. Be sure to download the 32-bit version of each component.
3. If prompted, restart the system.
4. Verify that the Exchange Management Tools can communicate with the Exchange 2007 mail server.

5. Follow site-specific procedures to install Microsoft Exchange Server 2007 Service Pack 1.
6. Install antivirus software. See Administering antivirus software on page 54
7. For completing the installation, perform the procedures in Completing the MMCW configuration on page 214.

Installing third-party software for Exchange 2003

When prompted to install third-party software:

1. Insert the customer-provided Microsoft Exchange Server media in the MAS drive.
2. Install the Management Tools by completing the Microsoft Exchange Installation wizard.
3. If you receive a compatibility warning, click **Continue**.
4. For details about this procedure, see the Microsoft Exchange documentation.
5. Install Microsoft Exchange Service Pack 2 and additional software downloads.
6. Installing antivirus software. See Administering antivirus software on page 54.
7. For completing the installation, perform the procedures in Completing the MMCW configuration on page 214.

Completing the MMCW configuration

After third-party software is installed, continue with the following steps to complete the configuration:

1. Verify that the *Avaya Modular Messaging Messaging Application Server Software* media in the MAS DVD drive. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
2. In the third-party dialog box, click **Continue with installation after installing 3rd-party software** on the 3rd-party dialog box. The MMCW resumes with the following sequence of events:
   - The **Setup** screen displays, followed by the **System Upgrade** screen.
   - The system restarts and logs on without user intervention.
   - MMCW restarts automatically and runs the MM Application Setup, installing all MM components.
   - After another restart and auto log on, the MMCW continues the system configuration, displaying informational messages, as each component, such as dialogic drivers or remote access is configured.
3. When MAS configuration is complete, the progress bar stretches across the window and the **Next** button becomes active. Click **Next**.

4. On the **Modular Messaging Wizard Completed** screen, click **Finish**.

Completing the server setup

To complete setup of the server complete the following tasks as necessary:

- Installing software updates on page 216
- Updating Microsoft Windows on page 217
- Verifying default LAN name and Power Management settings on page 217
- Entering RAS IP address on each MAS on page 218
- Setting logging location on page 219

Installing and configuring WebLM server

Use one of the following methods to install and configure the WebLM server:

- To install WebLM server on an MAS or a Supplementary server, proceed with Installing WebLM server on an MAS on page 90.
- If you already have a WebLM server that you are using for licensing other Avaya products, proceed with Obtaining the license file on page 91.
- To install WebLM server on a standalone server, see *Installing and configuring Avaya WebLM server* guide available on the Avaya Support Web site at http://www.avaya.com/support.

Installing software updates

The Modular Messaging Release 5.2 software is the most current version available at the time of release. However, you need to update the software after a migration to include the latest changes. Avaya provides these updates in the form of an Avaya Service Pack (SP) or a software patch.

To determine if a Modular Messaging software update is needed:

1. Locate any relevant Avaya software updates on the Avaya Support Web site at http://www.avaya.com/support. For complete steps, see Obtaining software updates from the Web on page 303.

   Note:

   If you followed the procedure for Downloading software updates on page 4, you would have already downloaded any required software updates.

If the Modular Messaging system requires a software update, do the update procedure now, before you do acceptance testing. Use the instructions in Appendix E: Updating Modular Messaging software on page 303 to update the system with the latest changes.

Updating Microsoft Windows

After a migration, 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.

Note:

Avaya technical support representatives must follow the specified internal procedures to verify the software that is installed. If required, the support representative must update the software with the latest patches as instructed.

Verifying default LAN name and Power Management settings

Rename the corporate LAN connection for this MAS so that it is easier to identify. To rename the LAN entry:

1. . Click **Start > Settings > Network Connections**.

   The **Network Connections** window opens.

2. Identify the corporate LAN on this server. The corporate LAN is labelled **Local Area Connection**.

   Rename this item as follows:

   a. Right-click the text **Local Area Connection** and select **Rename**.

   b. Change the name to **Corporate LAN**.

3. Change the Power Management settings for the LAN connection:

   a. Right-click the LAN connection and select **Properties**.

   b. Click **Configure**.

   c. Click the **Power Management** tab.

   d. Deselect the **Allow the computer to turn off this device to save power** checkbox.

4. Close any LAN-connection windows.

Entering RAS IP address on each MAS

The Avaya Modular Messaging Configuration wizard automatically sets up inbound remote access to each MAS modem. You must edit the preprogrammed RAS IP addresses to use the addresses that the technical support organization requires.

CAUTION:

If Avaya is to support this system, you must enter the RAS IP addresses assigned by the Avaya Automatic Registration Tool (ART). Otherwise remote access for Avaya technical support will not work.

Complete the following to set up the IP addresses on this MAS:

1. Double-click the **Configure** icon on the desktop.
2. In the left pane of the **Configure** window, expand **Routing and Remote Access**.
3. Expand the server name.
4. Verify authentication:
   a. Highlight **Remote Access Policies**.
   b. On the right pane, double-click **Connections to Microsoft routing and remote access**.
   c. Click the **Edit Profile..** button.
   d. Select the **Authentication** tab.
   e. Make sure that all check boxes (except for the **Unauthenticated access** check box) are selected. If necessary, clear the **Unauthenticated access** check box.
   f. Click **OK**.
   g. If a dialog box appears, click **No**.
   h. Click **OK**.
5. Right-click the server name from the pop-up menu and select **Properties**.
6. Set up PAP security:
   a. In the **Local Properties** window, click the **Security** tab.
   b. Click **Authentication Methods...**
   c. Select **Unencrypted Password (PAP)**.
   d. Verify that all other check boxes are blank. If necessary, clear the check boxes.
   e. Click **OK**.
7. Set up a static IP address pool as follows:
   a. In the local **Properties** window, click the **IP** tab.
   b. Under **IP address assignment**, select **Static address pool**.

c. Add or edit the address range as follows:

- If the window shows an incorrect IP address range, select the displayed range and click **Edit**.

CAUTION:

If Avaya Modular Messaging is to support this MAS, do not use the preprogrammed IP addresses. You must Edit and Remove these addresses for remote access to work.

- If no address range is already entered, click **Add**.

d. In the **Address Range** dialog box, enter the correct start and end IP addresses for this server.To get the start and end IP addresses, you *must* register your system.

e. Verify that the number of addresses is **2**.

f. Click **OK**.

g. In the **Adapter** field, select **Allow RAS to select adapter**.

h. Click **OK** to close the **Properties** window.

i. If a dialog box appears, click **No**.

j. Close the **Configure** window.

Setting logging location

CAUTION:

You must have adequate space on the drive where your logs are located. If you do not, your system may fail to operate correctly. Check the location where your system is recording logs to be sure you don't overrun your allotted space.

You may want to change the default location for recording logs, if you do not have adequate space on the default *C:* drive location. Likewise, if you installed Modular Messaging to a drive other than the default *C:* drive, the logging location is not automatically changed. In this case you may want to change the location for recording logs to the same drive as the software installation.

To change the location for recording logs, complete the following steps:

1. Navigate to the following location on the drive where Modular Messaging was installed: **<*drive*>:\Avaya_Support\Tools**.
2. Double-click the **MM_Logging.exe** file.

   The Modular Messaging **Verbose Logging** Window opens.
3. Complete the following steps for each type of log displayed at the top of the screen with the exception of the **Client**.

   a. Click the log-type button.

b. In the **Folder for Log Files:** field, edit the drive letter to the drive where you want logs stored. If you have installed Modular Messaging to an alternate drive, edit the field to show the drive where Modular Messaging was installed.

c. Click **Apply** at the bottom of the screen.

4. When the log location has been changed for all log types, click **Close** at the bottom of the screen.

The MM Debug Log Viewer should be set up to open log files automatically after installation. If for some reason this association is not made or it becomes changed, do the following manual setup.

To manually set up MM Debug Log Viewer:

1. From the desktop, open **My Documents** (or any Windows Explorer window).
2. Click **Tools > Folder Options > File Types**.
3. Is LOG4 listed in the extensions list?
   - If YES, skip to step 7.
   - If NO, continue with step 4.
4. Click **New**.
5. In the **Create New Extension** box, type **log4**. Click **OK**.
6. In the extensions list, at the top, highlight **LOG4**. Click **Change**.
7. Click **Select the program from a list**.
8. In the **Open With** window, highlight **MM Debug Log Viewer**. If this selection is not present, click **Browse** and navigate to and select **`C:\AVAYA_Support\Tools\LogViewer\MMLogViewer.exe`**.
9. Click **OK**.
10. Close all windows.

Disabling the customer-provided server

You need to disable the customer-provided server that is being replaced.

To disable the server:

- Busying out ports on page 221
- Logging off all remote logins on page 221
- Disabling services on page 222

Busying out ports

Busy out the ports on the MAS that you are replacing and on the switch.

To busy out the ports:

1. The PBX administrator must use the procedures appropriate for this PBX to busy out the ports. Depending on the switch integration, the administrator might be able to temporarily reroute calls to other MASs. If an MAS is unavailable, callers into the system might hear ring-no answer or a busy signal.
2. Use the port monitor to disable the MAS ports:
   a. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Port Monitor**.
   b. In the **Port Monitor** window, hold down the **Shift** key or Control (**Ctrl**) key and click to select all the ports.
   c. Right-click the port list and select **Disable**.
   d. Verify that the status of all ports is **Disabled**.
   e. Close the **Port Monitor** window.

Logging off all remote logins

To log off all remote logins:

1. Logon to the MAS using an account that has administrative permissions.
2. Click **Start** > **Programs** > **Administration**.
3. Open your **Windows Task Manager** and select the **Users** tab.
4. Select remote logins and click **Logoff**.
5. If there are no remote logins, click **Cancel** to exit.

Disabling services

You need to disable the services on the servers you want to replace from the existing system. See Disabling Modular Messaging services you plan to move on page 255 for more information.

Completing the migration

To complete the migration of the customer-provided server you need to:

- Move the services from the server that is being replaced to the new customer-provided server. See Moving Modular Messaging services among servers on page 257 for more information.
- Restore the customer data, see Restoring the customer-provided MAS on page 338.

  Note:

  However, you need not restore the caller apps as it is already restored during the installation of the new Modular Messaging system on the VMD.

  For more information, refer to the *Avaya Modular Messaging Documentation* library.
- Test the Modular Messaging system. For more information, see Chapter 7: Testing and backing up the system on page 107.

  CAUTION:

  Continue with the next step only if the new system has been completely tested and signed off by the customer.
- Remove the servers that you are replacing. To remove the servers:

  1. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration** to open the **VMSC window**.
  2. In the **VMSC** window, double-click **Message Application Servers**.
  3. Right-click the name of the server you are removing. Click **Remove**.
- Remove the Modular Messaging components from the server. For more information, see Appendix H: Removing Modular Messaging components from an MAS on page 327.
- Power off the servers you are removing.
- You need to repeat the procedure from Analyzing the existing system on page 206 for each MAS you need to migrate.

Appendix A: Installation, upgrade, and migration checklists

This appendix contains checklists to help guide you through the various installation, upgrade, and migration tasks.

- Before starting a new Modular Messaging installation, upgrade, or migration, print the checklist relevant to the procedure that you must do.
- Check off the steps as you complete them to make sure that you do not overlook any important tasks.

Checklists include:

- New installation:
  - New Modular Messaging installation on an Avaya MAS on page 226
  - New Modular Messaging installation on a customer-provided MAS on page 230
- Upgrade from Release 3.x or Release 4.0 to Release 5.2:
  - Modular Messaging upgrade on an Avaya MAS on page 236
  - Modular Messaging upgrade on a customer-provided MAS on page 241
- Migrate Modular Messaging to Release 5.2:
  - Modular Messaging migration on an Avaya MAS on page 245
  - Modular Messaging migration on a customer-provided MAS on page 249

New Modular Messaging installation on an Avaya MAS

This checklist applies to a new Modular Messaging installation using an Avaya Messaging Application Server (Avaya MAS). As you complete a procedure, make a check mark in the " ✔ " column.

Modular Messaging on an Avaya MAS installation checklist

✔	Description	Page	Comments
Complete preinstallation planning:			
	If Avaya is to maintain this system, preregister. The registration process produces product IDs for the servers and IP addresses for remote access.		You can obtain all required information for each MAS in advance.
	Assemble and review the required documentation.	2	Web access required.
	Download required software updates, including the latest version of the DCT executable file (**MMDCT.exe**) and client software.	4	Web access required.
	Obtain the DCT data file (**.mmdct)* for this site.	3	
	Review security considerations.	6	
	Obtain virus-checking software for the MAS if required.	6	Customer obtains.
	Gather the necessary test equipment and tools.	7	
	Arrange for initial switch and LAN administration. Register corporate FQDNs on the DNS if required. **Note:** Avaya is not responsible for the installation, administration, or test of communications between customer computers and the LAN.	8	See LAN administrator. Time of administration and site requirements vary.
	Verify that the switch or PBX is administered.	8	See switch administrator.
	Arrange for the Active Directory data schema update.	N/A	Review requirements in Chapters 4 and 5.
	Collect any software media that is needed for the installation, such as MS Windows updates or antivirus software.	4	Leave customer CDs and DVDs on-site.
Prepare to install the Modular Messaging software: Note: The customer Active Directory administrator may be required to perform these tasks.			
1 of 5			

Modular Messaging on an Avaya MAS installation checklist

✔	Description	Page	Comments
	Create the Modular Messaging customer account security group and customer account on the Active Directory server.	10	
	Create the technical support account on the Active Directory server.	10	
	Create test subscriber accounts on the Active Directory server (set up at least one for each TUI used on the site).	14	
	Assign permissions to the service permissions group.	17	
	Add a computer account for each MAS to the Active Directory server.	31	
	Set up each server for remote access.	32	
	Install the Active Directory and data schema updates for Windows 2003.	33	Do this before installing other Modular Messaging software. System restart required.
	Assign permissions with Exchange 2010	19	
	Configure NSPI for Windows Server 2008 Domain Controllers	36	
	Install the Modular Messaging Exchange subscriber administration extensions on any machine used to administer subscribers (and on Exchange server if required).	35	
Configure a new Avaya MAS:			
	Display an MAS from the console	48	
	Use the Avaya Modular Messaging Configuration wizard to access the DCT data file (**.mmdct)* to configure the MAS information automatically.	49	
	Install the User Administration Extensions at this time onto the Messaging Application Server.	40	
	Update Windows Internet Explorer 7 security.	51	
2 of 5			

Modular Messaging on an Avaya MAS installation checklist

✔	Description	Page	Comments
	For an Exchange 2003 system, install third-party software: • Exchange System Management Tools • Exchange Server 2003 SP2 (see comment) • antivirus software	51	
	For an Exchange 2007 system, install the following third-party software: • MAPI Client • Exchange 2007 Management Tools • Exchange Server 2007 SP1 • Additional components as prompted by installation • antivirus software For an Exchange 2010 system, install the following third-party software: • MAPI Client v6.5.8190or later • PowerShell 2.0 • Additional components as prompted by the installation • Antivirus software	51	
	Complete the MMCW configuration.	53	
	Administer antivirus software.	54	
	Install software updates.	55	
	Update Microsoft Windows.	62	
	Changing LAN settings	55	
	Enter RAS IP addresses on each MAS	56	
Configure the voice mail system: Note: The customer domain administrator may be required to perform these tasks.			
	Specify languages and verify that the Modular Messaging services are started.	81	For a non-English Windows operating system.
3 of 5			

Modular Messaging on an Avaya MAS installation checklist

✔	Description	Page	Comments
	Configure TUI and access settings.	82	Configuration notes required.
	Configure the broadcast mailbox.	83	
	Configure the PBX type.	86	
	Configure serviceability settings.	86	
	Install and configure the WebLM server	89	
	Obtain and apply PLDS license for this system.	91,91	
	Configure specific features: • Call Me service • Notify Me • MWI service • Languages or TTS • Audit service • MM Fax Service • Offline access to messages	93	Configure features as needed.
	Configure MAS-specific parameters: • INADS alarming (if used) • Port boards and switch integration	99	
	Restart service.	102	
	Verify call-handling capability.	104	
	Verify alarming setup.	104	
	Verify Tracing Service operation.	105	
	Verify Audit Service.	106	
	Repeat installation for any additional MASs.		
Test and back up the system:			
	Add a test subscriber on the directory server for each TUI used at this site.	108	
	Set up monitoring tools: • Operational History Viewer • Port monitor	110	
4 of 5			

Modular Messaging on an Avaya MAS installation checklist

✔	Description	Page	Comments
	Perform acceptance tests: • Create and send a call-answer message. • Retrieve test messages in integrated mode. • Create and send a test message in nonintegrated mode. • Test the outcalling capability. • Create and print a fax message • Run additional tests.	112	Repeat for each MAS that is set up to handle calls.
	Remove the test subscribers from the directory server.	118	
	Perform a complete DCT analysis of the supplementary server and all MASs.	119	
	Back up the system. Turn the system over to the customer.	119 120	Use local procedures. Be sure to give the customer an updated DCT data file.
	5 of 5		

New Modular Messaging installation on a customer-provided MAS

Use this checklist to install a new Modular Messaging system on a customer-provided MAS. As you complete a task, make a check mark in the " ✔ “column.

Modular Messaging on a customer-provided MAS installation checklist

✔	Description	Page	Comments
Complete preinstallation requirements:			
	If Avaya is to maintain this system, preregister the system in ART. The registration process produces product IDs for the servers and IP addresses for remote access.		You can obtain all required information for each MAS in advance.
	Assemble and review the required documentation.	2	Web access required.
	1 of 6		

Modular Messaging on a customer-provided MAS installation checklist

✔	Description	Page	Comments
	Download required software updates, including the latest version of the DCT executable file (**MMDCT.exe**) and client software.	4	Web access required.
	Obtain the DCT data file (**.mmdct*) for this site.	3	
	Review security considerations.	6	
	Obtain virus-checking software for the MAS if required.	6	Customer obtains.
	Gather the necessary test equipment and tools.	7	
	Arrange for initial switch and LAN administration. Register MAS corporate FQDNs on the DNS if required. **Note:** Avaya is not responsible for the installation, administration, or testing of communications between customer computers and the LAN.	8	See LAN administrator. Time of administration and site requirements vary.
	Verify that the switch or PBX is administered.	8	See switch administrator.
	Arrange for the Active Directory data schema update.	N/A	Review requirements in Chapters 4 and 5.
	Collect any software media that is needed for the installation, such as MS Windows updates or antivirus software.	4	Leave customer CDs and DVDs on-site.
Prepare to install the Modular Messaging software: Note: The customer Active Directory administrator may be required to perform these tasks.			
	Create the Modular Messaging customer account security group and customer account on the Active Directory server.	10	
	Create the technical support account on the Active Directory server.	10	
	Create test subscriber accounts on the Active Directory server (set up at least one for each TUI used on the site).	14	
	Assign permissions to the service permissions group.	17	
2 of 6			

Modular Messaging on a customer-provided MAS installation checklist

✔	Description	Page	Comments
	Add a computer account for each MAS to the Active Directory server.	31	
	Set up each server for remote access on the Active Directory server.	32	
	Install the Active Directory and data schema updates for Windows 2003.	33	Do this before installing other Modular Messaging software. System restart required.
	Install the Modular Messaging Exchange subscriber administration extensions on any machine used to administer subscribers (and on Exchange server if required).	35	
Configure a new MAS: Note: The customer domain administrator may be required to perform these tasks.			
	Make sure that you have the required hardware, software, and forms.	60	
	Run recommended disk checks: • Disk Defragmenter system tool • **chkdsk** command	62	
	Join the server to the MS Windows domain.	67	
	Adjust the following system values: • Event Viewer values • File and Printer Sharing properties • Windows Server 2003 operating system values	62	
	Add the Modular Messaging customer and technical support accounts to the local administrators group for this MAS.	68	
	Install and enable the following Windows software: • Required MS Windows services • MS Windows SP2 (if not already on the server)	64	Requires Microsoft Windows media.
	Install and run the Modular Messaging Configuration wizard.	69	
	Select a DCT data file (*.*mmdct*).	70	
3 of 6			

Modular Messaging on a customer-provided MAS installation checklist

✔	Description	Page	Comments
	Install the User Administration Extensions at this time onto the Messaging Application Server.	40	
	Update Windows Internet Explorer 7 security, if necessary.	72	
	For a system with an Exchange 2003 peer mail server, install third-party software: • Exchange System Management Tools • Exchange Server 2003 SP2 (see comment) • antivirus software	73	
	For a system with an Exchange 2007 peer mail server, install the following third-party software: • MAPI Client • Exchange 2007 Management Tools • Exchange Server 2007 SP1 • Additional components as prompted by installation • antivirus software For an Exchange 2010 system, install the following third-party software: • MAPI Client v6.5.8190 or later • PowerShell 2.0 • Additional components as prompted by the installation • Antivirus software	73	
	Complete the MMCW configuration.	74	
	Install software updates.	75	
	Update Microsoft Windows.	62	
	Verify power management settings	75	
	Enter RAS IP addresses on each MAS	76	
	Set the logging location if other than default.	77	
	Administer antivirus software.	54	
	Configure port boards.	309	
Configure the voice mail system: Note: The customer domain administrator may be required to perform these tasks.			
4 of 6			

Modular Messaging on a customer-provided MAS installation checklist

✔	Description	Page	Comments
	Specify languages and verify that the Modular Messaging services are started.	81	For a non-English Windows operating system.
	Configure TUI and access settings.	82	Configuration notes required.
	Configure the broadcast mailbox.	83	
	Configure the PBX type.	86	
	Configure serviceability settings.	86	
	Install and configure the WebLM server	89	
	Obtain and apply PLDS license for this system.	91,91	
	Configure specific features: • Call Me service • Notify Me • MWI service • Languages or TTS • Audit Service • MM Fax Service • Offline access to messages	93	Configure features as needed.
	Configure MAS-specific parameters: • INADS alarming (if used) • Port boards and switch integration	99	
	Restart service.	102	
	Verify call-handling capability.	104	
	Verify alarming setup.	104	
	Verify Tracing Service operation.	105	
	Verify Audit Service	106	
	Repeat for any additional MASs.		
Test and back up the system:			
	Add a test subscriber on the directory server for each TUI used at this site.	108	
5 of 6			

Modular Messaging on a customer-provided MAS installation checklist

✔	Description	Page	Comments
	Set up monitoring tools: • Operational History Viewer • Port monitor	110	
	Perform acceptance tests: • Create and send a call-answer message. • Retrieve test messages in integrated mode. • Create and send a test message in nonintegrated mode. • Test the outcalling capability. • Create and print a fax message • Run additional tests.	112	Repeat for each MAS that is set up to handle calls.
	Remove the test subscribers from the directory server.	118	
	Perform a complete DCT analysis of the supplementary server and all MASs.	119	
	Back up the system.	119	Use local procedures.
	Turn the system over to the customer.	120	Be sure to give the customer an updated DCT data file.
6 of 6			

Modular Messaging upgrade on an Avaya MAS

Use this checklist when you upgrade a system with an Avaya MAS that is running Modular Messaging Release 3.x or 4.0 to Modular Messaging Release 5.2. As you complete a procedure, make a check mark in the " ✔ " column.

Note:

If you are adding a new MAS to an existing Modular Messaging system, do the software upgrade first if an upgrade is required. When the upgrade is complete, install the new MAS using the appropriate new installation checklist.

Modular Messaging Avaya MAS upgrade checklist

✔	Description	Page	Comments
Complete pre-upgrade tasks:			
	Assemble and review the required documentation.	5	Web access required.
	Collect any software media that is needed for the upgrade, such as MS Windows updates or antivirus software.	4	Leave customer CDs and DVDs on-site.
	Schedule downtime for the Exchange server for updating the Modular Messaging Exchange extensions.	127	
	Download required software updates, including the latest version of the DCT executable file (**MMDCT.exe**) and client software.	130	Web access required.
	Review the considerations for a multiple-MAS upgrade.	127	
	Switch the monitor to show the correct server.	127	
	Verify and save key settings on the MAS. Record the following: • RAS IP addresses for each MAS • Non-default port groups and their names • MM services running on each MAS • SNMP trap destination and community details from the **Serviceability — Voice Mail Domain window**	128	
	1 of 5		

Modular Messaging Avaya MAS upgrade checklist

✔	Description	Page	Comments
	For Release 3.0 upgrade only, record all personal operator schedules.	129	
	If you use this MAS to create, administer, and deploy caller applications, back up all working files to a location other than the MAS. Additionally, ensure that you have on the MAS a current backup of the Caller Apps folder that contains the deployed caller applications that the MAS uses when it is running. Back up all customized tone files, customized prompt files, licensing files, WSO files, and SIP certificates for SIP implementations. Also back up the system state and spool.	129	
	Review configuration notes for any changes that might be needed regarding board configuration, switch programming, and application configuration. Make any necessary changes as part of the upgrade.	129	
	Check for errors or warnings on the system. Resolve major and minor alarms.	129	
	Set expectations and review product functionality with customer.	130	
	Install and configure WebLM server	89	
	Obtain and apply PLDS license for this system	91,91	
	Use a DCT data file (*.*mmdct*), using the DCT executable file (**MMDCT.exe**) to analyze each MAS.	130	
	Busy out the ports for this MAS.	132	Use PBX procedures.
	Back up the MAS.	132	
	Run recommended disk checks: • Disk Defragmenter system tool • **chkdsk** command	133	
	Log off all remote logins	133	
	Stop Modular Messaging services.	133	
2 of 5			

Modular Messaging Avaya MAS upgrade checklist

✔	Description	Page	Comments
	Update Windows Internet Explorer 7 security	134	
Upgrade software:			
	Upgrade RealSpeak software	135	Perform this step if you are upgrading from Release 3.x to 5.2.
	Start Modular Messaging services	136	
	Upgrade Dialogic drivers	136	
	Upgrade MAS software.	137	
Complete server setup:			
	Administer antivirus software.	139	
	Install software updates.	140	
	Update MS Windows.	140	
	Enable ports.	140	
Complete the upgrade:			
	If you have more than one MAS: • Let MAS#1 run for 15 minutes. • Upgrade each additional MAS.	141	
	Configure MM Fax server.	96	Perform this step if you are upgrading from Release 3.x to 5.2.
	Configure Audit service and verify its operation.	96	Perform this step if you are upgrading from Release 3.x to 5.2.
	Configure and activate additional new Release 5.2 features using the Voice Mail Configuration program.	92	
3 of 5			

Modular Messaging Avaya MAS upgrade checklist

✔	Description	Page	Comments
	Configure the SNMP trap destination and community details using the **Serviceability - Voice Mail Domain** window of the Voice Mail System Configuration program. Enter the SNMP trap destination and community information you recorded before beginning the upgrade.	141	
	Verify all personal operator schedules.	141	Perform this step if you are upgrading from Release 3.0 to 5.2.
	When finished with each MAS, verify that all Modular Messaging services that are required for this MAS are running.	112	
	Update Modular Messaging Active Directory Exchange extensions on any machines where they are installed.	127	
	Update client software on any non-MAS machines where it is installed.	254	As required.
Test and back up the system:			
	Add a test subscriber on the directory server for each TUI used at this site.	108	
	Set up monitoring tools: • Operational History Viewer • Port monitor	110	
	Perform acceptance tests: • Create and send a call-answer message. • Retrieve test messages in integrated mode. • Create and send a test message in nonintegrated mode. • Test the outcalling capability. • Create and print a fax message • Run additional tests.	112	Repeat for each MAS that is set up to handle calls.
	Remove the test subscribers from the directory server.	118	
	Back up the system.	119	Use local procedures.
4 of 5			

Modular Messaging Avaya MAS upgrade checklist

✔	Description	Page	Comments
	Run recommended disk checks: • Disk Defragmenter system tool • **chkdsk** command	119	
	If you are adding a new MAS to the system, begin the installation.	141	
	Turn the system over to the customer.	120	Be sure to give the customer an updated DCT data file.
5 of 5			

Modular Messaging upgrade on a customer-provided MAS

Use this checklist when you upgrade a system with a customer-provided server that is running Modular Messaging Release 3.x or 4.0 to Modular Messaging Release 5.2. As you complete a procedure, make a check mark in the " ✔ " column.

Note:

If you are adding a new MAS to an existing Modular Messaging system, do the software upgrade first if an upgrade is required. When the upgrade is complete, install the new MAS using the appropriate new installation checklist.

Modular Messaging customer-provided server upgrade checklist

✔	Description	Page	Comments
Complete pre-upgrade tasks:			
	If the Exchange extensions must be updated, schedule downtime for the Exchange server.	149	If required.
	Collect any software media that is needed for the upgrade, such as MS Windows updates or antivirus software.	147	Leave customer CDs and DVDs on-site.
	Assemble and review the required documentation.	147	Web access required.
	Install and configure WebLM server	89	
	Obtain and apply PLDS license for this system	91,91	
	Download required software updates, including the latest version of the DCT executable file (MMDCT.exe) and client software.	147, 4	Web access required.
	Review the considerations for a multiple-MAS migration.	150	
	Verify and save key settings on the MAS. Record the following: • RAS IP addresses for each MAS • Non-default port groups and their names • MM services running on each MAS • SNMP trap destination and community details from the **Serviceability — Voice Mail Domain window**	151	
	Record all personal operator schedules. (Release 3.0 upgrade only.)	151	
1 of 4			

Modular Messaging customer-provided server upgrade checklist

✔	Description	Page	Comments
	Back up caller-applications files on a non-MAS PC.	152	
	Review configuration notes for any changes that might be needed regarding board configuration, switch programming, and application configuration. Make any necessary changes as part of the upgrade.	152	
	Back up all caller applications, customized tone files, customized prompt files, licensing files, WSO files, and SIP certificates for SIP implementations. Also back up the system state and spool.	152	
	Check for errors or warnings on the system. Resolve major and minor alarms.	152	
	Set expectations and review product functionality with customer.	152	
	Run recommended disk checks: • Disk Defragmenter system tool • **chkdsk** command	155	
	Use a DCT data file (**.mmdct*) by using the DCT executable file (**MMDCT.exe**) to analyze each MAS.	152	The DCT data file serves as a backup but is not required for the upgrade. All MASs and Exchange message store must be running normally.
	Busy out the ports for this MAS.	154	Use PBX procedures.
	Back up the MAS.	155	
	Log off all remote logins	155	
	Stop all Modular Messaging services.	156	
	Install MS Windows prerequisite components	156	
	Update Windows Internet Explorer 7 security	157	
Upgrade software:			
	Upgrade RealSpeak software.	158	
	Start Modular Messaging services	159	
2 of 4			

Modular Messaging customer-provided server upgrade checklist

✔	Description	Page	Comments
	Upgrade Dialogic drivers.	159	
	Upgrade MAS software.	161	
	Install software updates.	163	
	Disable unused MS Windows services on this MAS.		Optional.
	Enable ports.	164	
Complete the upgrade:			
	If you have more than one MAS: • Let MAS#1 run for 15 minutes. • Upgrade each additional MAS.	165	
	Enable and configure MM Fax sender server.	96	
	Configure Audit service and verify its operation.	96	
	Configure and activate additional new Release 5.2 features.		
	Configure the SAL destination and community details using the **Serviceability - Voice Mail Domain** window of the Voice Mail System Configuration program. Enter the SAL destination and community information you recorded before beginning the upgrade.	165	
	Verify all personal operator schedules. (Release 3.0 upgrades only.)	141	
	When finished with each MAS, verify that all Modular Messaging services that are required for this MAS are running.	112	
	Update the Modular Messaging Active Directory Exchange extensions software on any machines where it is installed (including the Exchange server).	149	Most extension updates require a system restart.
	Update client software.	254	Do on each subscriber machine where client software is installed.
3 of 4			

Modular Messaging customer-provided server upgrade checklist

✔	Description	Page	Comments
	For any MAS that does not have Web Subscriber Options installed, close TCP port 80 to increase system security.	165	
Test and back up the system:			
	Add a test subscriber on the directory server for each TUI used at this site.	108	MM Aria is the default.
	Set up monitoring tools: • Operational History Viewer • Port monitor	110	Optional.
	Perform acceptance tests: • Create and send a call-answer message. • Retrieve test messages in integrated mode. • Create and send a test message in nonintegrated mode. • Test the outcalling capability. • Create and print a fax message • Run additional tests.	112	Do on each MAS that is set up to handle calls.
	Remove the test subscribers from the directory server.	118	
	Back up the system.	119	Use local procedures.
	Run recommended disk checks: • Disk Defragmenter system tool • **chkdsk** command	120	
	Turn the system over to the customer.	120	Be sure to give the customer an updated DCT data file.
4 of 4			

Modular Messaging migration on an Avaya MAS

Use this checklist when you migrate a system with an Avaya MAS that is running Modular Messaging Release 3.x, Release 4.0, or Release 5.1 to Modular Messaging Release 5.2. As you complete a procedure, make a check mark in the " ✔ " column.

Note:

If you are adding a new MAS or a supplementary server to an existing Modular Messaging system to the migrated Modular Messaging system, do the migration of the system first. When the migration is complete, add the new MAS or the supplementary server to the migrated system.

Modular Messaging Avaya MAS migration checklist

✔	Description	Page	Comments
Preparing for the migration:			
	If the Exchange extensions must be updated, schedule downtime for the Exchange server.	173	If required.
	Collect any software media that is needed for the upgrade, such as MS Windows updates or antivirus software.	170	Leave customer CDs and DVDs on-site.
	Assemble and review the required documentation.	170	Web access required.
	Download required software updates, including the latest version of the DCT executable file (**MMDCT.exe**) and client software.	170, 4	Web access required.
	Review configuration notes for any changes that might be needed regarding board configuration, switch programming, and application configuration. Make any necessary changes as part of the upgrade.	172	
	Obtain the Exchange System Management Tools and appropriate Service Pack from the customer.	170	
	Verify and save key settings on the MAS. Record the following: • RAS IP addresses for each MAS • Non-default port groups and their names • MM services running on each MAS • SAL destination and community details from the **Serviceability — Voice Mail Domain window**	176	
1 of 4			

Modular Messaging Avaya MAS migration checklist

✔	Description	Page	Comments
	Record all personal operator schedules.	176	
	Add the MAS to the system.	172	
	If you use this MAS to create, administer, and deploy caller applications, back up all working files to a location other than the MAS.	177	
	Back up all caller applications, customized tone files, customized prompt files, licensing files, WSO files, and SIP certificates for SIP implementations. Also back up the system state and spool.	177	
	Check for errors or warnings on the system. Resolve major and minor alarms.	177	
	Review product functionality with customer.	177	
	Change the switch integration type to SIP.	172	
	Disable and move the Modular Messaging services.	172	
	Test and back up the new MASs.	173	
	Remove the old MASs from the VMD.	173	
	Consideration for multiple-MAS migration.	173	
	Analyze the existing system.	176	
	Verify and save data.	176	
	Backup the MAS.	177	
Configuring the S8800 1U server:			
	Add the new S8800 1U server to the VMD.	178	
	Update the Microsoft Windows Internet Explorer security	181	
	Install and configure WebLM server	89	
	Obtain and apply PLDS license for this system	91,91	
	Install the User Administration Extensions at this time onto the Messaging Application Server.	40	
	Install third-party software.	181	
2 of 4			

Modular Messaging Avaya MAS migration checklist

✔	Description	Page	Comments
	Complete the MMCW configuration.	183	
	Stop all Modular Messaging services	190	
Complete MAS configuration:			
	Administer antivirus software	183	
	Install Modular Messaging software updates.	185	
	Update MS Windows.	186	
	Disable the private LAN	186	
	Enter RAS IP addresses on each MAS	186	
	Busy out the ports for this MAS.	189	Use PBX procedures.
	Disable Modular Messaging services	190	
Complete the migration:			
	Move the services.	190	
	Restore the data.	190	
	Back up each MAS.	169	
	Power off the server.	190	
Testing and backing up the system:			
	Add a test subscriber for each TUI used at this site.	108	
	Set up monitoring tools: • Operational History Viewer • Port monitor	110	
	Perform acceptance tests: • Create and send a call-answer message. • Retrieve test messages in integrated mode. • Create and send a test message in nonintegrated mode. • Test the outcalling capability. • Run additional tests.	112	
	Remove the test subscribers.	118	
3 of 4			

Modular Messaging Avaya MAS migration checklist

✔	Description	Page	Comments
	Perform a complete DCT analysis of all MASs and the Supplementary server.	169	
	Back up the system.	119	
	Run recommended disk checks: • Disk Defragmenter system tool • **chkdsk** command	120	
	Turn the system over to the customer.	120	
4 of 4			

Modular Messaging migration on a customer-provided MAS

Use this checklist when you migrate a system with a customer-provided MAS that is running Modular Messaging Release 3.x, Release 4.0, or Release 5.1 to Modular Messaging Release 5.2. As you complete a procedure, make a check mark in the " ✔ " column.

Note:

If you are adding a new MAS or a supplementary server to an existing Modular Messaging system to the migrated Modular Messaging system, do the migration of the system first. When the migration is complete, add the new MAS or the supplementary server to the migrated system.

Modular Messaging customer-provided server migration checklist

✔	Description	Page	Comments
Prepare for the migration:			
	If the Exchange extensions must be updated, schedule downtime for the Exchange server.	196	If required.
	Collect any software media that is needed for the upgrade, such as MS Windows updates or antivirus software.	194	Leave customer CDs and DVDs on-site.
	Assemble and review the required documentation.	194	Web access required.
	Download required software updates, including the latest version of the DCT executable file (**MMDCT.exe**) and client software.	194	Web access required.
	Review the configuration notes.	195	
	Obtain the Exchange System Management Tools and appropriate Service Pack from the customer.	194	
	Verify and save the data, run recommended disk checks and verify a DCT data file (**.mmdct*).	196	
	Back up the MAS to be replaced.	196	
	Add the customer-provided MAS to the system.	196	
	Switch the monitor to show the correct server.	201	
1 of 4			

Modular Messaging customer-provided server migration checklist

✔	Description	Page	Comments
	Verify and save key settings on the MAS. Record the following: • RAS IP addresses for each MAS • Non-default port groups and their names • MM services running on each MAS • SAL destination and community details from the **Serviceability — Voice Mail Domain window**	206	
	Change the switch integration type to SIP	205	
	Disable and move the Modular Messaging services.	196	
	Test and backup the new MASs.	196	
	Remove the old MASs from the VMD.	196	
	Consideration for multiple-MAS migration.	196	
Prepare customer-provided server:			
	Install Microsoft Windows 2003.	197	
	Set the computer name.	199	
	Configure network card.	200	
	Run recommended disk checks.	200	
	Install modem drivers.	200	
Set up the customer-provided server:			
	Join the Windows domain	201	
	Adjust system values	202	
	Add the Modular Messaging accounts to the Administrator groups.	204	
Install Microsoft Windows services:			
	Install Microsoft Windows 2003 SP2	199	
Migrate each MAS:			
	Analyze the existing data.	206	
2 of 4			

Modular Messaging customer-provided server migration checklist

✔	Description	Page	Comments
	Verify and save data U	206	
	Back up each MAS	207	
	Run the MMCW configuration.	208	
	Update the Windows Internet Explorer 7 security.	212	
	Install third-party software	212	
	Complete the MMCW configuration.	214	
Complete the MAS configuration:			
	Install and configure WebLM server	89	
	Obtain and apply PLDS license for this system	91,91	
	Administer antivirus software.	214	
	Install Modular Messaging software updates	216	
	Update Microsoft Windows software	217	
	Verify Power Management settings.	217	
	Enter RAS IP addresses on each MAS	218	
	Set logging locations.	219	
	Busy out the ports for this MAS.	221	
	Disable Modular Messaging services.	222	
Complete the migration:			
	Move the services	223	
	Restore the data	223	
	Back up each MAS	193	
	Power off the server	223	
Test and back up the system:			
	Add a test subscriber for each TUI used at this site.	108	
3 of 4			

Modular Messaging customer-provided server migration checklist

✔	Description	Page	Comments
	Perform acceptance tests: • Create and send a call-answer message. • Retrieve test messages in integrated mode. • Create and send a test message in nonintegrated mode. • Test the outcalling capability. • Create and print a fax message • Run additional tests.	112	Do on each MAS that is set up to handle calls.
	Remove the test subscribers from the directory server.	118	
	Perform a complete DCT analysis of all MASs and the Supplementary server.	193	
	Back up the system.	119	Use local procedures.
	Run recommended disk checks: • Disk Defragmenter system tool • **chkdsk** command	120	
	Turn the system over to the customer.	120	Be sure to give the customer an updated DCT data file.
4 of 4			

Appendix B: Post-installation procedures for Modular Messaging

This appendix describes how to configure the Modular Messaging system after the installation is complete.

This appendix contains three procedures:

Updating client software: The Modular Messaging client software packages must be updated on each subscriber machine where they are already installed.

Converting Supplementary server to run a 0 port MAS on the Supplementary server: This procedure should be performed by a technician on the site to convert supplementary server to run 0 port MAS.

Changing switch integration: Perform this procedure on the site to change switch integration after an upgrade of the MAS, if required.

Topics in this appendix include:

- Updating client software on page 254
- Disabling Modular Messaging services you plan to move on page 255
- Moving Modular Messaging services among servers on page 257
- Enabling the services on the correct server on page 263
- Completing the move services procedure on page 266
- Converting Supplementary server to run a 0 port MAS on the Supplementary server on page 267
- Changing switch integration on page 269

Updating client software

Note:

Always check the Avaya Support Web site at http://www.avaya.com/support for the latest Modular Messaging Client software package.

Do this task on each subscriber machine where client software is installed.

The Modular Messaging client software packages must be updated on each subscriber machine where they are already installed.

To update the client software to the latest release, use the normal software installation procedures for this site. For example:

1. If you have not already done so, download the most recent version of the client software package from the support website. When you download the software, copy it to a USB storage device.
2. Insert the USB storage device with the client software into any USB port on the subscriber machine where a Modular Messaging client software package from the previous release is installed.
3. Log on to the subscriber machine. You must use an account with administrator rights to install software (such as the local administrator account for the client machine).
   a. Navigate to the directory where you saved the client software on the USB storage device.
   b. Double-click the **setup.exe** file.
   c. The Avaya Modular Messaging Client Installation wizard runs. Follow the prompts.
4. Repeat this procedure until all existing versions of client software have been replaced with the latest version for the release.

For details on installing or using a client software package, see the appropriate user guide.

Disabling Modular Messaging services you plan to move

Before you move any Modular Messaging services, you must disable the service to be moved on the server where it is currently running.

CAUTION:

You must set any **MM** services that you intend to move to another server to **Disabled** before you enable them on a different server. Serious problems occur if you activate a service that is supposed to run on only one server in the VMD on multiple servers.

To disable services to be moved on the server where the service is currently running:

1. Log on to each server that you intend to move Modular Messaging services from.
2. Double-click the **Monitor** icon on the desktop.
3. Click **Services (Local)** in the left pane.
4. In the right pane of the Monitor window, scroll down to the service you plan to move.
   a. Right-click the service and select **Stop**.
   b. Double-click the service to open the **Properties** window.
   c. Set the **Startup type** to **Disabled**.
   d. Click **OK**.
5. Repeat Step 4 to disable each service you intend to move. Services you can move include:
   - MM Call Me—must be on the same server with the Mailbox Monitor Server
   - MM Mailbox Monitor—must be on the same server with either Call Me or MWI
   - MM MWI—must be on the same server with the Mailbox Monitor Server
   - MM Fax Sender Service —enable on a server with voice ports that support Fax calls
   - MM Auditing Service—enable on each server in the VMD
   - MM Tracing Server—must be enabled on only one server at a time in the VMD
6. Refresh the screen to verify that all **MM** services that you plan to move are **Disabled**.
7. Repeat this procedure on the next MAS, if the Modular Messaging services to be moved reside on more than one server.
8. If you are moving Fax Sender service, complete the following steps to stop sharing the Microsoft Fax Printer on the MAS the service is being moved from:
   a. Click **Start** > **Settings** > **Printers and Faxes**.
   b. In the **Printers and Faxes** window, right-click the Fax and select **Properties**.
   c. Click the **Sharing** tab.

d. Remove the check from the **Share this printer** check box and click **OK**.

e. Exit all windows.

Moving Modular Messaging services among servers

To move services:

1. Log on to the supplementary server you intend to move Modular Messaging services to.
2. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration**.
3. Move the following services as required:
   - Moving Call Me, MWI, and Mailbox Monitor on page 257
   - Moving MM Fax Sender service on page 259
   - Moving Audit service on page 261
   - Moving Tracing Server service on page 261

Moving Call Me, MWI, and Mailbox Monitor

You must enable the Call Me Server, Message Waiting Indicator (MWI) Server, and Mailbox Monitor services only once in the voice mail domain. All three services must be enabled on the same server, or serious problems will occur.

Updating the Call Me Server

To change the Call Me Server parameters:

1. Under the voice mail domain, such as *vmdom*, double-click **Call Me**.
2. In the Call Me - Voice Mail Domain window, on the **General** tab, click the check box to **Enable Call Me**.
3. For **MAS Call Me Server**, specify the server on which to enable the Call Me service:
   a. Click the **...** button next to the field.
   b. In the **Select Computer** window, double-click the name of the supplementary server.
   c. Click **OK** to close this window.

   Note:

   Because Call Me Server and Message Waiting Indicator (MWI) Server both use the Mailbox Monitor Server, you must enable both services on the same server.

Updating the MWI Server

To change the Message Waiting Indicator (MWI) Server parameters:

1. Under the voice mail domain double-click **Message Waiting Indicator**.
2. In the **Message Waiting Indicator - Voice Mail Domain** window, on the **General** tab, click the check box to **Enable Message Waiting Indicator (MWI)**.
3. For **MAS MWI server**, specify the server on which to enable the MWI Server:
   a. Click the **...** button next to the field.
   b. In the **Select Computer** window, double-click the name of the server.
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** box, list all MASs that have a port group set up to support MWI. To add a server name:
   a. Double-click inside the top of the big list box, or click the **Add** button just above 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 each MAS that has ports allocated to support MWI.
   d. Repeat Steps b and c to add any other MASs that support MWI.
   e. Click **OK** to close the **Select Computer** window.

   Note:

   The arrow icons move the selected MAS up or down the list. MWI requests start with the first MAS in the list, and continue to each additional MAS if needed.
6. Click **OK** to close this window.

Updating the MAS port groups

Update the MAS port groups as required:

1. In the **Voice Mail System Configuration** window, expand **Message Application Servers**.
2. Expand the entry for this MAS.
3. Double-click **Port Groups**. Update the values as required.

   For example, you might move all the MWI ports to the new server. Depending on the integration type, you might leave the MWI ports that are already active enabled. You can then add MWI ports to the new server to increase the ports available for MWI.
4. If required, expand the entries for the other servers in the system. Return to Step 2, and update the **Port Groups** for each server as required.

Moving MM Fax Sender service

The supplementary server is **not** an Avaya-recommended location for the fax service as it is recommended for the fax service to run on a system that has voice boards. IP H.323 switch integration does not support fax service. To move MM Fax Sender service:

- Enable MM Fax Sender service on the new location
- Remove the MM Fax Printer from the old location
- Share the MM Fax Printer on the new location
- Stop MM Fax Sender on the old location
- Start MM Fax Sender on the new location
- Configure dialing rules on the new location
- Configure the new MM Fax Sender server using VMSC

Enable MM Fax Sender service on the MAS that will now host MM Fax Sender service:

1. Run **C:\Avaya_Support\Utils\FaxSenderEnable.exe** on the MAS that will now host MM Fax Sender.
2. Restart the Microsoft Fax Service.

Remove the MM Fax Printer from the MAS that will no longer host MM Fax Sender service:

1. Click **Start > Settings > Printers and Faxes**.
2. In the Printers and Faxes window, right-click the Fax and select **Properties**.
3. Click the **Security** tab.
4. Remove the Network Service user.
5. Click the **Sharing** tab.
6. Remove the **Share this printer** check from the check box.
7. Click the **Security** tab.
8. Remove any Fax permissions.

Share the MM Fax Printer on the MAS that will now host MM Fax Sender:

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. Click the **Share this printer** check box. Leave the share name as Fax.
8. Click the **Security** tab.
9. Verify that **Everyone** is assigned Fax permissions on the share.

Complete the following steps to assign permissions to the Fax Service Manager:

1. Select 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. Ensure that **Everyone** is assigned **Fax** permissions for the Fax Service Manager.
8. Exit all windows.

Note:

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

Start MM Fax Sender on the MAS that will now host it:

1. Disable MM Fax Sender on the server that was previously running it; see Disabling Modular Messaging services you plan to move on page 255
2. Open the Monitor window on the MAS that will now host MM Fax Sender.
3. Click **Services (Local)** in the left pane, if the item is not already selected.
4. In the right pane, scroll down to **MM Fax Sender Server**.
5. Right-click **MM Fax Sender Server** and select **Start**.
6. Double-click **MM Fax Sender Server** to open the Properties window.
7. Set the **Startup type** to **Automatic**.
8. Click **OK** and then close the Monitor window.

Create the Phone and Modem dialing rule on the MAS that will now host MM Fax Sender:

1. On the on the MAS that will now host MM Fax Sender, 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.
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**.

Configure MM Fax Sender on the new location:

1. In the **Voice Mail System Configuration** window, under the voice mail domain, such as *vmdom*, double-click **Fax**.
2. In the Fax - Voice Mail Domain window, on the **General** tab:
   a. Next to **MM Fax Sender server,** click **Browse**.
   b. In the **Select Computer** window, enter the name of the MAS you now chose as your MM Fax Sender server.
   c. Click **Check Names**.
   d. Click **OK** to accept the MAS name and close the window.
3. Click **OK** to close the **Fax - Voice Mail Domain** window.
4. On the "restart" window, click **OK**.

Moving Audit service

Audit service is installed on each MAS in the VMD. Complete the following steps to change the MAS that will act as the MM Audit Server:

1. Under the voice mail domain double-click **Auditing**.
2. In the **Auditing - Voice Mail Domain** window, on the **General** tab, click the check box to **Enable Auditing**.
3. In the **Audit server** field, enter the name of the server that you want to run the MM Audit service, or use the browse button (...) to select the name.
4. In the **Database server** field, enter the name of the server where the database resides or use the browse button (...) to select the server.
5. Click **OK** to close this window.

Moving Tracing Server service

To move the Tracing Server service to a different server:

1. Log on to the supplementary server that you intend to move the Tracing Server service to.

   Note:

   You must have already disabled the Tracing Server service on the server that was previously running it. For more information, see Disabling Modular Messaging services you plan to move on page 255.

2. Enable the new instance of the Tracing Server service:
   a. Double-click the **Monitor** icon on the desktop.

b. Click **Services (Local)** in the left pane.

c. In the right pane, scroll down to the list of Modular Messaging services.

d. Double-click the **MM Tracing Server** service to open the **Properties** window.

1. Set the **Startup type** to **Enabled**.
2. Click **OK**.

e. In the Monitor window, right-click **MM Tracing Server** and select **Start**.

3. Access the Voice Mail System Configuration program. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Voice Mail System Configuration**.
4. Under the voice mail domain double-click **Tracing System**.
5. The system displays a warning that the current Home Message Application Server is not valid. Click **OK**.
6. In the **Tracing System - Voice Mail Domain** window, on the **General** tab:
   - The **MAS Tracing Server Machine Name** field displays the name of the server that is now running the tracing system. The new server can be an MAS or a supplementary tracing server.
   - The **Home Message Application Server** field shows the first MAS that the tracing system connects to when doing an operation. You do not have to update this field.
7. Click **OK** to close this window.
8. Remove the scheduled tasks from the server that previously hosted the Tracing Service:

   a. Click **Start** > **Run** to open the Run window.

   b. In the **Open** field, type the following and press **Enter**:

   C:\Avaya_Support\Tools\Tracing\RemoveSchedTasks.exe

   CAUTION:

   This script automatically removes the tasks that were assigned to the original tracing server, so you do not have to set up the scheduled tasks again on the new server. If you fail to run this script after you move Tracing Service from one server to another, errors occur when the originally scheduled tasks fail.

Enabling the services on the correct server

After you set up the services correctly in the VMSC, you must enable the services on the appropriate servers. You must stop all Modular Messaging services to do this task.

Stopping all Modular Messaging services

You must stop all Modular Messaging services on all servers that you are moving services to or from. Stopping and then restarting all services gets the entire voice mail domain configured with the correct services running on the correct servers.

To stop all Modular Messaging services:

1. Switch the monitor to show the first MAS.
2. Stop all Modular Messaging services as follows:
   a. Click **Start** > **Run** to open the Run window.
   b. In the **Open** field, type the following and press **Enter**:

      C:\Avaya_Support\Tools\ServiceControl\StopMMServices.exe

      A command window displays the status of the Modular Messaging services shutdown. The script might take several minutes to complete.

      Note:

      This script also stops Dialogic services and some Windows services.
3. Confirm that all Modular Messaging services are stopped:
   a. Double-click the **Monitor** icon on the desktop.
   b. Click **Services (Local)** in the left pane.
   c. In the right pane, scroll down to the list of installed Modular Messaging services. These all start with the abbreviation **MM**.
   d. Verify that the **Status** column is blank. If any service is *not* stopped, repeat Steps 2 and 3.
4. Repeat this procedure on each server that you are moving services to or from.

Enabling the appropriate services

After all Modular Messaging services are stopped, you must enable the appropriate services on each server. To enable the appropriate Modular Messaging services:

1. In the Monitor window, click **Services (Local)** in the left pane.

2. In the right pane, scroll down to the list of Modular Messaging services. These services start with the abbreviation **MM**.

   CAUTION:
   Verify that you enable and disable the correct services on the supplementary server. Enable some Modular Messaging services only once in a voice mail domain, or serious problems will occur. For more information, see Table 5.

Table 5: When to enable Modular Messaging services in a VMD

Modular Messaging service name	Condition for enabling service [1]
MM Messaging Application Server	Enable on each MAS and supplementary server.
MM Alarming Server MM Audit Service MM Event Monitor Server MM Fault Monitor MM Performance Monitor Server MM Process Monitor Server MM Service Connector	Enable this set of services on each server in the voice mail domain.
MM Call Me [2] MM Fax Server[3] MM Mailbox Monitor [2] MM MWI [2] MM Tracing Server	Enable this set of services *only once* in each voice mail domain, either on an MAS or on the supplementary tracing server. Enable MM Fax Server on a server with voice ports that support Fax calls.

1. Each enabled service must have a startup type of **Automatic** and show a status of **Started**.
2. The Call Me, MWI, and Mailbox Monitor services always must be enabled on the same server.
3. Fax Sender service must be co-resident with the MM Fax Service Provider (MM FSP).

3. To enable an **MM** service on this server:
   a. Double-click the service to open the Properties window.
   b. Set the **Startup type** to **Automatic**.
   c. Click **OK**.
   d. Repeat Step 3 to update the status for each MM service as required.
4. To disable an **MM** service on this server:
   a. Double-click the service to open the Properties window.
   b. Set the **Startup type** to **Disabled**.
   c. Click **OK**.
   d. Repeat Step 4 to update the status for each MM service as required.

5. Refresh the screen. Verify that the **Status** column shows the correct state for each Modular Messaging service.
   - Services that are required for this server must show a startup type of **Automatic**.
   - Services that are *not* required on this server must show a blank status and a startup type of **Disabled**.

   CAUTION:

   You must set all **MM** services to the correct state before you restart Modular Messaging services. Serious problems occur if you activate a service that is supposed to run on only one server in the VMD on multiple servers.
6. Repeat this procedure on each server that you are moving services to or from.

Restarting messaging service

After you verify and update all required settings on all servers in the voice mail domain, you must restart the services on each server.

To restart messaging service:

1. Click **Start** > **Run** to open the Run window.
2. 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.
3. Refresh the screen to verify that all **MM** services required for this server are **Started** and set to **Automatic**.
4. If any required **MM** services are not set up correctly, return to Enabling the appropriate services on page 263. Correct the problem, and then restart service again.
5. Restart all Modular Messaging services on each Modular Messaging server in the voice mail domain after you finish moving services. A restart ensures that the voice mail domain-wide properties are consistent across the VMD.

Completing the move services procedure

To complete the procedure for moving Modular Messaging services:

1. Verify basic server operation and do the appropriate acceptance tests. For more information, see Chapter 7: Testing and backing up the system on page 107.
2. Because you moved Modular Messaging services, the DCT data file currently on the system is now out of date. To update the system configuration data:
   a. Use the most recent DCT data file, which is on your USB storage device.
   b. Use the DCT executable file (**MMDCT.exe**) to analyze all the servers in the system again. For more information.
3. Update and turn over the DCT data file. Send a copy of the most current DCT data file to the appropriate technical support group. Afterwards, erase the copy of the DCT data file from your USB storage device.

Converting Supplementary server to run a 0 port MAS on the Supplementary server

This section is optional, you only need to complete this procedure if your Modular Messaging support organization has advised you to do so.

Use the following steps on the Supplementary server to convert the Supplementary server to run a 0 port MAS on the Supplementary server:

Note:

These steps only need to be completed on supplementary severs, which have been upgraded to Modular Messaging Release 5.1.

1. Run the registry file, ***C:\Avaya_Support\Registry_Keys\convertsupp_2_0portmas.reg.***
2. Set the MM MAS service to **Automatic**. *Do not* start the service at this time.
3. Make sure that the MM Service Connector service is set to **Automatic**. *Do not* start the service at this time.
4. Make sure that the MM Fault Monitor service is set to **Automatic.** Do not start the service at this time.
5. Make sure that the following MM Alarming Services are set to **Automatic**:
   - MM Alarming Server
   - MM Event Monitor Server
   - MM Performance Monitor Server
   - MM Process Monitor Server

   Do not start the services at this time.
6. Locate and run ***gvconfig.exe***:
   a. Locate and run ***C:\Program Files\Avaya Modular Messaging\VServer\Config\ gvconfig.exe*** file.
   b. When prompted, enter the name of the **Peer Message Storage Server** for your system.
   c. Click **Next**.
   d. When prompted, select **Subsequent Server** in an existing VMD
   e. Click **Next**.
   f. Enter the LDAP Security Password for your Modular Messaging system.
   g. Click **Next**.
   h. Click the name of your MM VMD from the drop-down list.
   i. Click **Next**.

j. If the system prompts you to install missing prompts, insert the **Avaya Modular Messaging R5.1 MAS Application DVD 1 of 2** disk in to the Supplementary server DVD drive. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".

k. Click **Next**.

l. Select the **Skip Caller Application deployment** check box.

m. Click **Next**.

n. Click **Next** on **User Information** screen.

   This **User Information** screen remains displayed and disabled while user information is populated on the server. The time taken to populate the user information depends on the number of users supported by the MM System.

o. Click **Finish**.

7. Double-click the ***C:\Avaya_Support\Tools\ServiceControl\StopMMServices.exe*** file to stop all MM services.
8. Double-click the ***C:\Avaya_Support\Scripts\serverrecovery.vbs*** file to start all MM services.

Changing switch integration

This topic describes how to change the switch integration after an upgrade. This assumes you only change the switch integration type of the MASs and that MAS servers remain the same. These procedures vary with the type of switch integration involved:

- Changing from DSE or Analog to QSIG on page 269
- Changing from DSE or QSIG to H.323 on page 270
- Changing from DSE or QSIG to SIP on page 272
- Changing from QSIG T1 to QSIG E1 on page 273
- Changing from H.323 to SIP on page 274

If changing from H.323 to QSIG, contact support for instructions.

Changing from DSE or Analog to QSIG

The following explains how to change from the DSE or Analog switch integration to the QSIG switch integration:

1. Upgrade all MASs in the Voice Mail Domain (VMD) to Release 5.2 as explained in this chapter.
2. Using VMSC, complete the following changes to the switch integration and telephony interface settings for the MAS you plan to move to QSIG:
   a. Set Switch Integration to **None**.
   b. Set number of ports to **0**.
3. Set all MM services that are running on the MAS to Manual:
   a. Double-click the **Monitor** icon on the desktop or from command prompt, run ***services.msc***.
   b. Select **Services (Local)** in the left pane.
   c. In the right pane, scroll down to the list of Modular Messaging services.

      These services start with the abbreviation **MM**.
   d. Double-click the service to open the **Properties** window.
   e. Set the **Startup type** to **Manual**.
   f. Click **OK**.
   g. Repeat this procedure for all appropriate **MM** services.
4. Shut down the MAS.

5. Remove the Dialogic boards from the MAS.

   See the *Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions* for board removal and installation.

6. Start the MAS without any Dialogic boards installed.
7. Shut down the MAS.
8. Install the Dialogic QSIG boards into the MAS and connect the QSIG trunks to each Dialogic board.
9. Start the MAS.
10. Configure the boards using DCM; see Configuring port boards on page 309.
11. Start the MAS service:
    a. Once configured, double-click the **Monitor** icon on the desktop or from command prompt, run ***services.msc***.
    b. Select **Services (Local)** in the left pane, if the item is not already selected.
    c. In the right pane, scroll down to **MM Messaging Application Server**.
    d. Right-click **MM Messaging Application Server** and select **Start**.
12. Using VMSC, configure the Switch Integration and the telephony interface settings for the MAS to match the recommended settings in the QSIG Switch Configuration note (for note information, see the Avaya Support Web site at http://www.avaya.com/support).
13. Restart the messaging service and set all services to **Automatic**; see Restarting messaging service on page 265.
14. Test the QSIG integration; see Verifying call-handling capability on page 104.
15. Repeat steps 2 through 14 for each of the remaining MASs you are moving to a QSIG integration.
16. After you confirm that the new switch integration is working on the MASs, create and verify the DCT for all MASs in your VMD; see Using the DCT to collect information from an MAS on page 130.

Changing from DSE or QSIG to H.323

The following explains how to change from the DSE or QSIG switch integration to the H.323 switch integration:

1. Upgrade all MASs in the Voice Mail Domain (VMD) to Release 5.2 as explained in this chapter.
2. Using VMSC, complete the following changes to the switch integration and telephony interface settings for the MAS you plan to move to H.323:
   a. Set Switch Integration to **None**.

b. Set number of ports to **0**.

3. Set all MM services that are running on the MAS to Manual:
   a. Double-click the **Monitor** icon on the desktop or from the command prompt, run ***services.msc***.
   b. Select **Services (Local)** in the left pane.
   c. In the right pane, scroll down to the list of Modular Messaging services.

      These services start with the abbreviation **MM**.
   d. Double-click the service to open the **Properties** window.
   e. Set the **Startup type** to **Manual**.
   f. Click **OK**.
   g. Repeat this procedure for all appropriate **MM** services.
4. Shutdown the MAS.
5. Remove the Dialogic boards from the MAS.

   See the *Avaya Modular Messaging S8730-Family Hardware Maintenance and Additions* for board removal.
6. Start the MAS.
7. Start the MAS service:
   a. Double-click the **Monitor** icon on the desktop or from command prompt, run ***services.msc***.
   b. Select **Services (Local)** in the left pane, if the item is not already selected.
   c. In the right pane, scroll down to **MM Messaging Application Server**.
   d. Right-click **MM Messaging Application Server** and select **Start**.
8. Using VMSC, configure the Switch Integration and the telephony interface settings for the MAS to match the recommended settings in the H.323 Switch Configuration note (for note information, see the Avaya Support Web site at http://www.avaya.com/support).
9. Restart the messaging service and set all services to **Automatic**; see Restarting messaging service on page 265.
10. After the messaging service has restarted and the system has produced the NT Application 1241 event, run the utility **`C:\Avaya_Support\Tools\ConfigureMMIPSEC\ConfigureMMIPSEC.exe`**
11. Test the H.323 integration; see Verifying call-handling capability on page 104.
12. Repeat steps 2 through 14 for each of the remaining MASs you are moving to a H.323 integration.
13. After you confirm that the new switch integration is working on the MASs, create and verify the DCT for all MASs in your VMD; see Using the DCT to collect information from an MAS on page 130.

Changing from DSE or QSIG to SIP

The following explains how to change from the DSE or QSIG integration to the SIP switch integration:

1. Create and verify the DCT for all MASs in your VMD; see Using the DCT to collect information from an MAS on page 130.

   You will not be changing the Switch Integration type at this time.

2. Upgrade all MASs in the Voice Mail Domain (VMD) to Release 5.2 as explained in this chapter.
3. After completing the upgrade, use WebLM admin to apply your new Modular Messaging Release 5.2 license, which includes the SIP certificate. Then use VMSC to import the certificates. See Obtaining the license file on page 91 and Applying license file on the WebLM server on page 91.
4. Using VMSC, change the Switch Integration type to SIP for the MAS (start with MAS#1) and make all VMSC configuration changes as documented in the SIP Switch Integration Configuration note (for note information, see the Avaya Support Web site at http://www.avaya.com/support).
5. Using VMSC, change the number of ports for the MAS to the number of ports required with your SIP integration.
6. Restart the messaging service and set all services to **Automatic**; see Restarting messaging service on page 265.
7. After the messaging service has restarted and the system has produced the NT Application 1241 event, run the utility **`C:\Avaya_Support\Tools\ConfigureMMIPSEC\ConfigureMMIPSEC.exe`**
8. Test the SIP integration; see Verifying call-handling capability on page 104.
9. Shut down the MAS.
10. Remove the Dialogic boards from the MAS.

    See *Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions* guide for information on board removal.

11. Start the MAS without any Dialogic boards installed.
12. Ensure that all MM Services start up properly.
13. Repeat steps 4 through 12 for each MAS you plan to move to the SIP integration.
14. Create and verify the DCT for all MASs in your VMD; see Using the DCT to collect information from an MAS on page 130.

Changing from QSIG T1 to QSIG E1

The following explains how to change from the QSIG T1 to the QSIG E1 switch integration:

1. Upgrade all MASs in the Voice Mail Domain (VMD) to Release 5.2 as explained in this chapter.
2. Using VMSC, complete the following changes to the switch integration and telephony interface settings for the MAS you plan to move to QSIG:
   a. Set Switch Integration to **None**.
   b. Set number of ports to **0**.
3. Set all MM services that are running on the MAS to Manual:
   a. Double-click the **Monitor** icon on the desktop or from the command prompt, run ***services.msc***.
   b. Select **Services (Local)** in the left pane.
   c. In the right pane, scroll down to the list of Modular Messaging services.

      These services start with the abbreviation **MM**.
   d. Double-click the service to open the Properties window.
   e. Set the **Startup type** to **Manual**.
   f. Click **OK**.
   g. Repeat this procedure for all appropriate **MM** services.
4. Shutdown the MAS.
5. Remove the Dialogic boards from the MAS.

   See the *Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions* guide for information on board removal and installation.
6. Start the MAS without any Dialogic boards installed.
7. Shutdown the MAS.
8. Install the Dialogic QSIG E1 boards into the MAS and connect the QSIG E1 trunks to each Dialogic board.
9. Start the MAS.
10. Configure the boards using DCM; see Configuring port boards on page 309.

11. Start the MAS service:
    a. Once the port boards are configured, double-click the **Monitor** icon on the desktop or from the command prompt, run ***services.msc***.
    b. Select **Services (Local)** in the left pane, if the item is not already selected.
    c. In the right pane, scroll down to **MM Messaging Application Server**.
    d. Right-click **MM Messaging Application Server** and select **Start**.
12. Using VMSC, configure the Switch Integration and the telephony interface settings for the MAS to match the recommended settings in the QSIG E1 Switch Configuration note (for note information, see the Avaya Support Web site at http://www.avaya.com/support).
13. Restart the messaging service and set all services to **Automatic**; see Restarting messaging services on page 102.
14. Test the QSIG integration; see Verifying call-handling capability on page 104.
15. Repeat steps 2 through 14 for each of the remaining MASs you are moving to a QSIG integration.
16. After you confirm that the new switch integration is working on the MASs, create and verify the DCT for all MASs in your VMD; see Using the DCT to collect information from an MAS on page 130.

Changing from H.323 to SIP

The following explains how to change from the H.323 to the SIP switch integration:

1. Upgrade all MASs in the Voice Mail Domain (VMD) to Release 5.2 as explained in this chapter.
2. After completing the upgrade, use the WebLM admin to apply your new Modular Messaging Release 5.2 license, which includes the SIP certificate. Then use VMSC to import the certificates. See Obtaining the license file on page 91 and Applying license file on the WebLM server on page 91.
3. Using VMSC, change the Switch Integration type to SIP for the MAS (start with MAS#1) and make all VMSC configuration changes as documented in the SIP Switch Integration Configuration note (for note information, see the Avaya Support Web site at http://www.avaya.com/support).
4. Using VMSC, change the number of ports for the MAS to the number of ports required with your SIP integration.
5. Restart the messaging service and set all services to **Automatic**; see Restarting messaging services on page 102.
6. After the messaging service has restarted and the system has produced the NT Application 1241 event, run the utility **`C:\Avaya_Support\Tools\ConfigureMMIPSEC\ConfigureMMIPSEC.exe`**

7. Test the SIP integration; see Verifying call-handling capability on page 104.
8. Repeat steps 3 through 7 for each MAS in the VMD you plan to move to the SIP integration.
9. Create and verify the DCT for all MASs in your VMD; see Using the DCT to collect information from an MAS on page 130.

Appendix C: Creating a new tone file

This appendix describes how to build a tone file for Dialogic analog port boards by using the PBXpert utility to learn PBX tones.

Do this procedure after you administer the port boards on the switch, but before you configure the port boards using the Intel Dialogic product Configuration Manager. For more information, see Configuring analog port boards on page 314.

CAUTION:

Use the configuration notes for the PBX or switch integration to administer the port boards. For instructions on obtaining the configuration notes, see Downloading configuration notes on page 4. Administer the port boards on the switch before you can continue.

PBXpert learns the call progress tones for this PBX and stores in a Tone Set File (TSF). You can store many tone sets in a single TSF file.

You can use the PBXpert utility either automatically or manually:

- *Automatic Learning:* PBXpert uses two different channels on the Dialogic port board to set up tones and learn the resulting call progress tones automatically. To use this procedure, see Learning tones automatically on page 278.
- *Manual Learning:* PBXpert uses one channel on the Dialogic port board and a telephone to set up tones and learn the resulting call progress tones manually. PBXpert prompts you how and when to use the telephone. To use this procedure, see Learning tones manually on page 281.

  Note:

  If only one line is connected to the Dialogic port board, you must use Manual Learning.

Learning tones automatically

This section describes:

- Running the PBXpert wizard on page 278
- Consolidating and saving the TSF file on page 280
- Using the new TSF in Dialogic Configuration Manager on page 280

Running the PBXpert wizard

The PBXpert wizard guides you to learn the tones used by the PBX and saving the information as a TSF file. PBXpert can learn the following tones:

- Dial tone
- Ringback
- Busy
- Reorder (fast busy)
- Disconnect

To run the PBXpert wizard:

1. Start the Dialogic port boards:
   a. The Intel Dialogic product Configuration Manager window must be open.

      To open the DCM application, click **Start** > **Programs** > **Intel Dialogic System Release** > **Configuration Manager - DCM**.

   b. Click the green **Start** button on the button bar.

   When the service starts, the **Stop** button becomes active and the installed boards show a green light.
2. Click **Start** > **Programs** > **Intel Dialogic System Release** > **PBX Expert**.

   The PBXpert main window opens. Most fields are blank until tones are learned.

   - If you are using PBXpert for the first time after installation, the PBXpert wizard starts automatically.
   - If the PBXpert wizard does not start automatically, click **Tones** > **Tone Wizard**.

   Note:

   You can change the default settings in the wizard if you are familiar with this PBX environment and the Dialogic API. The program saves any settings that you change when you exit PBXpert. For help on a particular screen, click the **Help** button in the wizard.

After the PBXpert Wizard window opens, complete the screens as follows:

1. On the Welcome screen, click **Next**.
2. On the PBX Information screen:
   - Under **PBX**, enter the name of the **Manufacturer**, such as *Mitel*.
   - Enter the **Model** of the PBX, such as *SX-2000*.
   - You can use the automatically created **Tone Set File** name, or change the file name.
   - Click **Next**.
3. On the Select a Board screen:
   - Select the port board to use.
   - Click **Next**.
4. On the Select the Calling Resource screen, for the Line A (Calling Channel):
   - For **Select the Channel**, enter the port number or the channel to use.
   - For **Phone Number**, enter the extension number of this port.
   - Click **Next**.
5. On the Select the Called Resource screen, for the Line B (Called Channel):
   - For **Select the Channel**, enter a port number or the channel that is different from Line A.
   - For **Phone Number**, enter the extension number of this port.
   - Click **Next**.
6. On the Settings Confirmation screen:
   - Verify the settings. Click **Back** if you need to change anything.
   - Verify if you have checked the **Run Wizard Auto-Test** box.
   - Click **Next**.
7. The Auto Line Test window opens while PBXpert verifies the connection between the two specified channels.
   - If you see a **Test finished successfully!** message, click **OK**. Close this window and proceed.
   - If the line test fails:
     a. Click **OK**. Close this window.
     b. Click **Back**, adjust the settings, and try the test again.
8. On the Learning Tones screen, click **Next** to start learning tones automatically.

   The Learn Tones window opens.

   Note:

   You can click **Cancel** any time during the test to stop automated learning.

9. When PBXpert completes learning, choose to keep or discard the data.
   - If the tones were learned without errors, select **Keep Data**. The Learn Tones window closes and you can proceed.
   - If errors occurred, select **Discard Data**. The window closes.
     - Click **Back**, adjust the settings, and learn the tones again.
     - You cannot test or save the tone file if it contains errors.
10. On the Verifying the Learn screen, click **Next** to test the learned tones.
    - If the test succeeds, click **OK** to close the test window and proceed.
    - If the test fails, click **OK** to close this window. Click **Back** on the wizard, adjust the settings, and try the test again.
11. The Summary of Results screen shows the final wizard status and the tone definitions. Click **Finish**.

    The PBXpert main window displays the tone definitions.

Consolidating and saving the TSF file

You must consolidate and save the new TSF file so you can use it with the Dialogic voice driver. To do this:

1. Click **Tones** > **Consolidate**.
2. After consolidation is complete, click **File** > **Save** to save the new TSF file.
   a. In the Save As window, navigate to the **C:\Avaya_Support\Tone_Files** directory to ensure that you have saved the file.
   b. Specify a file name with file type of TSF, such as *Mitel-SX-2000.tsf*.

Using the new TSF in Dialogic Configuration Manager

To use the new TSF that you just created:

1. Return to the Intel Dialogic product Configuration Manager window.
2. Click the red **Stop** button on the button bar.
3. Return to Step 6 in Configuring analog port boards on page 314 and complete board configuration and testing.

Learning tones manually

This section describes:

- Running PBXpert on page 281
- Adding a new tone set on page 282
- Learning tone definitions on page 282
- Testing the tone set on page 283
- Consolidating and saving the TSF file on page 283
- Using the new TSF in Dialogic Configuration Manager on page 284

Running PBXpert

To run PBXpert manually:

1. Start the Dialogic port boards.
   a. The Intel Dialogic product Configuration Manager window must be open.

      To open the DCM application, click **Start** > **Programs** > **Intel Dialogic System Release** > **Configuration Manager - DCM**.

   b. Click the green **Start** button on the button bar.

   When the service starts, the **Stop** button becomes active and the installed boards show a green light.
2. Click **Start** > **Programs** > **Intel Dialogic System Release** > **PBX Expert**.

   The system opens the **PBXpert** main window. Most fields are blank until tones are learned. If you are using PBXpert for the first time after installation, the PBXpert wizard starts automatically.
3. Select the **Don't run wizard at startup** check box and then click **Cancel**.

   A new, empty TSF is now active.
4. In the PBXpert main window, click **Settings** on the button bar. The system opens the **Settings** window.
5. Click the Dialing tab, and complete the following:
   a. Under **Line A**, enter the **Board Number**, such as *1*.
   b. Enter the **Channel Number** or **Port number**.
   c. Verify that the **Manual mode** check box is checked.

d. For **Phone Number**, enter the extension for this port or channel.

You can use the default values for all other fields in this window. Click **Help** for more information if needed.

e. Repeat Steps a through d for **Line B**.

Note:

If you are familiar with this PBX environment and the Dialogic API, you can change these default settings. The program saves any settings that you change when you exit PBXpert.

f. Click **OK**.

Adding a new tone set

To add a new tone set to a TSF:

1. From the PBXpert main window, click **Edit** > **New Tone Set**.
2. In the New Toneset window:
   a. Enter the PBX **Manufacturer**, such as *Mitel*, and the **Model** name, such as *SX-2000*.
   b. Click **OK**.

   The **PBXpert** main window shows the manufacturer and model names you entered. The tone definitions are set to zero.

Learning tone definitions

To add tone definitions to the new tone set:

1. From the PBXpert main window, click **Tones** > **Learn**.
2. On the Start Learn window:
   a. Select the tones for the Dialogic boards to learn. The default is all tones.
   b. Click **Start Learn** to have PBXpert start learning tones.

   The Learn Tones window opens.

   Note:

   Click **Cancel** any time to stop learning.
3. The system prompts you to listen for ringing, and to pick up or replace the telephone handset, during the test. When a message box pops up, do the requested action, and then click **OK**.

4. When the learning process is complete, the system displays the tone definitions in the Learn Tones window. Choose to keep or discard the data:
   - If the tones were learned without errors, select **Keep Data**. The Learn Tones window closes and you can proceed.
   - If errors occurred, select **Discard Data**. The window closes.
     - Click **Back** on the wizard, adjust the settings, and try to learn the tones again.
     - You cannot test or save the tone file if it contains errors.

   The **Learn Tone** window closes. The **PBXpert** main window displays the new tone definitions.

Testing the tone set

The Test function verifies that the consolidated tone set in the active TSF works correctly with Perfect Call, a call progress analysis utility.

To test the newly learned tones:

1. In the main PBXpert window, click **Tones** > **Test**.
2. A Test window opens.

   When testing is complete, the Test window displays the test results.
3. Verify that the tone definitions of the learned tones are correct.

Consolidating and saving the TSF file

You must consolidate and save the new TSF file so you can use it with the Dialogic voice driver. To do this:

1. Click **Tones** > **Consolidate**.
2. Click **File** > **Save** to save the new TSF file.
   a. In the Save As window, navigate to the following directory to ensure that the file is backed up: **C:\Avaya_Support\Tone_Files**

   Note:

   If you use the default DATA directory, the system will *not* back up the customized tone file automatically.

   b. Specify a file name of TSF file type, such as *Mitel-SX-2000.tsf*.

Using the new TSF in Dialogic Configuration Manager

To use the new TSF that you just created:

1. Return to the Intel Dialogic product Configuration Manager window.
2. Click the red **Stop** button on the button bar.
3. Return to Step 6 in Configuring analog port boards on page 314 and complete board configuration and testing.

Appendix D: Installing Dialogic port boards in a customer-provided MAS

This appendix describes how to install Dialogic port boards and their drivers in a customer-provided server, also called a customer-provided MAS. A customer might have several servers that support Avaya Modular Messaging software and services.

CAUTION:

Modular Messaging Release 5.2 does not support Dialogic port boards with new Installations and migrations on Avaya-provided hardware or customer-provided hardware

- One to ten servers that handles call-processing functions. These are called *Messaging Application Server (MAS)* servers. An MAS can contain port boards, depending on the switch integration.
- One supplementary server that is configured like an MAS, but does not handle calls and does not contain port boards.
- Multiple optional servers that handle special services only. An optional server never contains port boards.

CAUTION:

Use the procedures in this chapter *only* to install Dialogic port boards into a customer-provided server that is to handle calls.

Continue with Chapter 2: Preparing to install Modular Messaging software on page 9 if:

- you are using Avaya-provided hardware, For detailed procedures, see *Installing the Avaya S8800 Server for Modular Messaging* guide or *Maintaining the Avaya S8730 Server* guide.
- this Avaya Modular Messaging system is to use an IP H.323 or IP SIP integration. These IP switch integration methods do not use port boards.

Note:

Before you can do the tasks described in this section, verify that all preinstallation requirements were met. See Chapter 1: Preinstallation requirements on page 1.

Topics in this chapter include:

- Supported MAS port boards on page 286
- Installing MAS port boards on page 287
- Connecting MAS port boards to the switch on page 300
- Completing the hardware installation on page 301
- Testing the port boards on page 317

Supported MAS port boards

Table 6 lists the Dialogic port boards that Avaya supports for all new installations that use customer-provided servers. The type of port boards required depends on the switch integration, but each MAS can have only one type of port board installed. For example, all the boards in the server must be T1-QSIG or DSE.

Table 6: Supported MAS port boards for customer-provided servers

Protocol	Ports per MAS	Port boards	Maximum Number	Dialogic files on documentation library
Analog	12 - 48	Dialogic D/120JCT-LS 12-port board	4	**D/120JCT-LS** (PDF)
	4 - 16	Dialogic D/41JCT-LS 4-port board	4	**D/41JCT-LS** (PDF)
Digital Set Emulation	8 - 16	Dialogic D/82JCT-U-PCI-UNIV Dialogic D/82JCT-EW	2	**D/82JCT-U PCI Univ** (PDF)
E1-QSIG	30 - 60	Dialogic D/600JCT-1E1 [1] or D/600JCT-2E1	2	**D/600JCT-1E1** or **D/600JCT-2E1** (PDF) **D/600JCT-1E1-120-EW**
T1-QSIG	23 - 46	Dialogic D/480JCT-1T1 [1] Dialogic D/480JCT-1T1- EW	2	**D/480JCT-1T1** (PDF) **D/480JCT-1T1-EW** (PDF)

1. Early D/600JCT-1E1 and D/480JCT-1T1 QSIG port boards have a plug in the unused connector on the faceplate. Dialogic D/600JCT-1E1 or D/480JCT-1T1 QSIG port boards that ship after mid-2005 have only a single connector. Both types of QSIG boards operate identically.

Note:

To support the capacities shown in Table 6, the minimum customer-provided server hardware specifications must match the specifications for the S8800 MAS. For more information, see the *Avaya Modular Messaging Concepts and Planning Guide*.

The Dialogic documents provide details about installing and connecting the port boards. The documents are available on the *Avaya Modular Messaging Documentation* library on www.avaya.com/support Web site. For instructions on how to obtain the documents, see Downloading required software and documentation on page 3. For the latest version of the Dialogic guides, see the Quick Install Cards Search Tool on the Intel Telecom Boards Web site.

Note:

The Dialogic documentation describes more setups than the ones used for Avaya Modular Messaging. If information in a Dialogic document conflicts with this Avaya document, follow the steps in the Avaya documentation. Use the Dialogic documentation to locate various items on the board or verify cable connections.

Installing MAS port boards

Do this task only on a customer-provided server.

Before you can install the Modular Messaging software on a customer-provided server, you must first install any required port boards in each MAS.

Note:

The number of port boards you can install in a customer-provided MAS depends on the type of board and the number of PCI slots in the server. These instructions assume that up to four PCI slots are available in the server, and that board installation starts with the fourth PCI slot. Modify these instructions as appropriate for the server that you are using.

Preparing for the installation

To install Dialogic port boards in a customer-provided MAS:

1. Verify that this MAS meets the minimum requirements needed to support Modular Messaging software. For more information, see the *Avaya Modular Messaging Concepts and Planning Guide*.
2. Print the appropriate Dialogic PDF file for more information. For a list of the Dialogic documents that support each type of board, see Table 6: Supported MAS port boards for customer-provided servers on page 286.
3. If the server is already in operation, take it out of service to install the port boards. Schedule and publicize a time.
4. When you are ready to start the installation, shut down the system software and turn off the server. Unplug the AC power cord for safety.

   CAUTION:

   Electrostatic discharge can severely damage sensitive electronic circuits. Before handling any electronic hardware, be sure to wear a grounding wrist strap or other static-dissipating device. The antistatic wrist strap must touch your bare skin and the strap cable must connect to an earth ground. For complete ESD instructions, see "Protecting against ESD damage" on the documentation library.
5. Open the chassis to access the PCI card slots.
6. Remove the cover for the PCI slot in which you want to install the new board. Set the retaining screw aside.
   - If you are installing multiple boards, remove as many card slot covers as are needed.
   - Note the maximum number of boards of a certain type that you can install in one MAS. See Table 6: Supported MAS port boards for customer-provided servers on page 286.

Note:

When you insert boards, start from the right-most slot if possible. For example, if six PCI slots are in the server, start with PCI slot 6 to insert the port boards.

Setting jumpers and switches

Set the jumpers and switches for board position, bus termination, and other features as described in this section. For more information about jumper or switch locations, see the Dialogic documentation listed in Table 6: Supported MAS port boards for customer-provided servers on page 286.

Note:

The Dialogic documentation describes more setups than the ones used for Avaya Modular Messaging. If information in a Dialogic document conflicts with this Avaya document, follow the steps in the Avaya documentation. Use the Dialogic documentation to locate various items on the board or verify cable connections.

To set the jumpers and switches on each board:

1. Remove the new port board from its packaging. Do not touch the circuit board surface.
2. Set the jumpers and switches as required for this type of board:
   - D/480JCT-1T1 and D/600JCT-1E1 or D/600JCT-2E1 QSIG board settings on page 289
   - D/480JCT-1T1-EW and D/600JCT-E1-120-EW QSIG board settings on page 289
   - D/82JCT-U PCI Univ set emulation board settings on page 290
   - D/82JCT-U EW set emulation board settings on page 291
   - D/120JCT-LS 12-port analog board settings on page 292
   - D/120JCT-LS-EW port analog board settings on page 292
   - D/41JCT-LS 4-port analog board settings on page 294
   - D/41JCT-LS-EW analog board settings on page 295

D/480JCT-1T1 and D/600JCT-1E1 or D/600JCT-2E1 QSIG board settings

To set up Dialogic T1 or E1 QSIG boards, you must set only the board ID for the port board.

1. Turn the rotary switch, located on the top of the port board. Set the board ID according to the slot number in which the board is installed.

   The Dialogic port boards usually are placed in the PCI slots starting from the right side of the cabinet. For the board ID numbers for a 6-PCI slot MAS, see Table 7.

Table 7: D/480JCT-1T1 and D/600JCT-1E1 or D/600JCT-2E1 QSIG board ID settings

Card number	Board ID number	PCI slot number
1	0	6
2	1	5

Note:

Do *not* set the Computer Telephony (CT) bus for bus termination.

2. Continue with Installing the port boards on page 298.

D/480JCT-1T1-EW and D/600JCT-E1-120-EW QSIG board settings

If a system has two boards, they must be installed in adjacent slots.

For the D/480JCt-1T1-EW and D/600JCT-E1-120-EW boards, set the board ID and turn off power budgeting.

1. Turn the rotary switch, located on the top of the port board. Set the board ID according to the slot number in which the board is installed.

The Dialogic port boards usually are placed in the PCI slots starting from the right side of the cabinet. For the board ID numbers for a 6-PCI slot MAS, see Table 7.

Table 8: D/480JCT-1T1-EW and D/600JCT-E1-120-EW QSIG board ID settings

Board ID number	PCI slot number
0	3
1	4

2. Move the P3 jumper on the top of the board on to pins 1-2 to disable power budgeting.

D/82JCT-U PCI Univ set emulation board settings

To set up Dialogic digital set emulation (DSE) boards, you must set only the bus termination.

1. If the server contains more than one port board, set the boards on both ends of the Computer Telephony (CT) bus for bus termination. Use jumper **P8** to set CT bus termination as shown in Table 9.

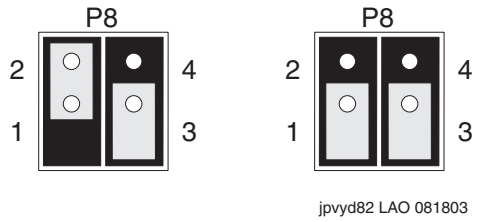
Table 9: D/82JCT-U set emulation board settings for CT bus termination

Number of cards	P8 jumper	CT bus termination
1	OFF	Do not terminate bus.
2	Card 1: ON pins 1 and 2 Card 2: ON pins 1 and 2	Terminate bus on both boards.
3	Card 1: ON pins 1 and 2 Card 2: OFF Card 3: ON pins 1 and 2	Terminate bus on boards 1 and 3.
4	Card 1: ON pins 1 and 2 Card 2: OFF Card 3: OFF Card 4: ON pins 1 and 2	Terminate bus on boards 1 and 4.

Figure 1 shows the **P8** jumper settings.

- The setting on the left is ON. Pins 1 and 2 are jumpered. If set, the CT bus is terminated.
- The setting on the right is OFF.

Figure 1: D/82JCT-U board settings for CT bus termination: ON or OFF



2. Continue with Installing the port boards on page 298.

D/82JCT-U EW set emulation board settings

To set up Dialogic digital set emulation (DSE) boards, you must set only the bus termination.

1. If the server contains more than one port boards, set the boards on both ends of the Computer Telephony (CT) bus for bus termination and turn off power budgeting on all boards. Use jumper **P8** to set CT bus termination as shown in Table 9.

Table 10: D/82JCT-U set emulation board settings for CT bus termination

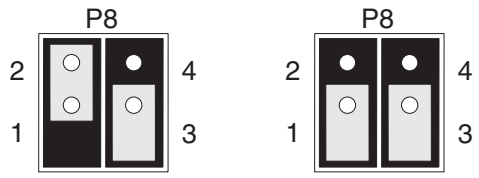
Number of cards	P8 jumper	CT bus termination
1	OFF	Do not terminate bus.
2	Card 1: ON pins 1 and 2 Card 2: ON pins 1 and 2	Terminate bus on both boards.

2. Set the P8 jumper to the appropriate position for the system configuration:
   - For a system with two boards, move the P8 jumper on to pins 1 and 2.
   - For a system with one board, verify that the P8 jumper is only on pin 1.

   Figure 2 shows the **P8** jumper settings.
   - The setting on the left is ON. Pins 1 and 2 are jumpered. If set, the CT bus is terminated.
   - The setting on the right is OFF.

Figure 2: D/82JCT-U board settings for CT bus termination: ON or OFF

z



3. Move the P11 jumper on the top of the board on to pins 1–2 to disable power.

D/120JCT-LS 12-port analog board settings

To set up Dialogic 12-port analog boards:

1. Set the unique board ID for the port board. Turn the rotary switch, located on the top of the board. Set the board ID according to the slot number in which the port board is installed.

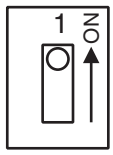
   The Dialogic port boards usually are placed in the PCI slots starting from the right side of the cabinet. For the board ID numbers for a 6-PCI slot MAS, see Table 11.

Table 11: D/120JCT-LS 12-port analog board ID settings

Card number	Board ID number	PCI slot number
1	0	6
2	1	5
3	2	4
4	3	3

2. Set the hook-switch state of the port board to **ON** so callers hear a busy signal when the board is not initialized. Use the **SW1** switch, located at the top of the board, to set the hook-switch state. See Figure 3.

Figure 3: D/120JCT-LS analog board setting for on-hook switch



jpvysw1 LAO 081803

3. Continue with Installing the port boards on page 298.

D/120JCT-LS-EW port analog board settings

Determine in which slot in the PCI cage you will be installing the board. Slots in the PCI cage are number 3 (bottom slot) 4 (middle slot) and 5 (top slot). If a system has two boards, they

must be installed in adjacent slots. For the D/120JCT-LS-EW board, set the board ID, the hook-switch state and turn off power budgeting.

1. Set the unique board ID for the port board. Turn the rotary switch, located on the top of the board. Set the board ID according to the slot number in which the port board is installed.

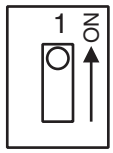
   The Dialogic port boards usually are placed in the PCI slots starting from the right side of the cabinet, see Table 12.

Table 12: D/120JCT-LS-EW port analog board ID settings

Board ID number	PCI slot number
0	3
1	4

2. Set the hook-switch state of the port board to **ON** so callers hear a busy signal when the board is not initialized. Use the **SW1** switch, located at the top of the board, to set the hook-switch state. See Figure 4.

Figure 4: D/120JCT-LS analog board setting for on-hook switch



jpvysw1 LAO 081803

3. Move the P3 jumper on the top of the board on to pins 1–2 to disable power budgeting.

D/41JCT-LS 4-port analog board settings

To set up Dialogic 4-port analog boards:

1. Set the unique board ID for the port board. Turn the **SW30** rotary switch, located on the top of the board. Set the board ID according to the slot number in which the board is installed.

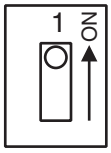
   The Dialogic port boards usually are placed in the PCI slots starting from the right side of the cabinet. For the board ID numbers for a 6-PCI slot MAS, see Table 13.

Table 13: D/41JCT-LS 4-port analog board ID settings

Card number	Board ID number	PCI slot number
1	0	6
2	1	5
3	2	4
4	3	3

2. Set the hook-switch state of the port board to **ON** so callers hear a busy signal when the board is not initialized. Use the red **SW4** switch, located near the top of the board, to set the hook-switch state. See Figure 5: D/41JCT-LS analog board setting for on-hook switch on page 294.

Figure 5: D/41JCT-LS analog board setting for on-hook switch



jpvysw1 LAO 081803

3. If the server contains more than one port board, set the boards on both ends of the Computer Telephony (CT) bus for bus termination. Use jumper **JP2** to set CT bus termination as shown in Table 14.

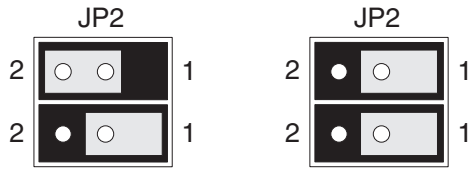
Table 14: D/41JCT-LS analog board settings for CT bus termination

Number of cards	JP2 jumper	CT bus termination
1	OFF	Do not terminate bus.
2	Card 1: ON pins 1 and 2 Card 2: ON pins 1 and 2	Terminate bus on both boards.
3	Card 1: ON pins 1 and 2 Card 2: OFF Card 3: ON pins 1 and 2	Terminate bus on boards 1 and 3.
4	Card 1: ON pins 1 and 2 Card 2: OFF Card 3: OFF Card 4: ON pins 1 and 2	Terminate bus on boards 1 and 4.

Figure 6 shows the **JP2** jumper settings.

- The setting on the left is ON. Pins 1 and 2 are jumpered. If set, the CT bus is terminated.
- The setting on the right is OFF.

Figure 6: D/41JCT-LS analog board settings for CT bus termination: ON or OFF



jpvyd41 LAO 081803

D/41JCT-LS-EW analog board settings

Determine in which slot in the PCI cage you will be installing the board. Slots in the PCI cage are number 3 (bottom slot) 4 (middle slot) and 5 (top slot). If a system has two boards, they must be installed in adjacent slots. For the D/41JCT-LS-EW board, set the board ID, the

hook-switch state and Computer Telephony (CT) bus termination. CT bus termination is set by adjusting the JP2 jumper on the side of the board.

1. Set the unique board ID for the port board. Turn the **SW30** rotary switch, located on the top of the board. Set the board ID according to the slot number in which the board is installed.

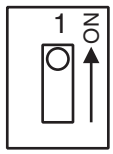
   The Dialogic port boards usually are placed in the PCI slots starting from the right side of the cabinet, see Table 15.

Table 15: D/41JCT-LS 4-port analog board ID settings

Board ID number	PCI slot number
0	3
1	4

2. Set the hook-switch state of the port board to **ON** so callers hear a busy signal when the board is not initialized. Use the red **SW4** switch, located near the top of the board, to set the hook-switch state. See Figure 7: D/41JCT-LS analog board setting for on-hook switch on page 296.

Figure 7: D/41JCT-LS analog board setting for on-hook switch



jpvysw1 LAO 081803

3. If the server contains more than one port board, set the boards on both ends of the Computer Telephony (CT) bus for bus termination. Use jumper **JP2** to set CT bus termination as shown in Table 16.

Table 16: D/41JCT-LS-EW analog board settings for CT bus termination

Number of cards	JP2 jumper	CT bus termination
1	OFF	Do not terminate bus.
2	Card 1: ON pins 1 and 2 Card 2: ON pins 1 and 2	Terminate bus on both boards.

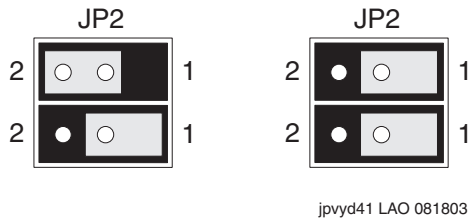
4. Set the JP2 jumper to the appropriate position for the system configuration:
   - For a system with two boards, move the JP2 jumper on to pins 1 and 2.

- For a system with one board, verify that the JP2 jumper is only on pin 1.

Figure 8 shows the **JP2** jumper settings.

- The setting on the left is ON. Pins 1 and 2 are jumpered. If set, the CT bus is terminated.
- The setting on the right is OFF.

Figure 8: D/41JCT-LS-EW analog board settings for CT bus termination: ON or OFF



Installing the port boards

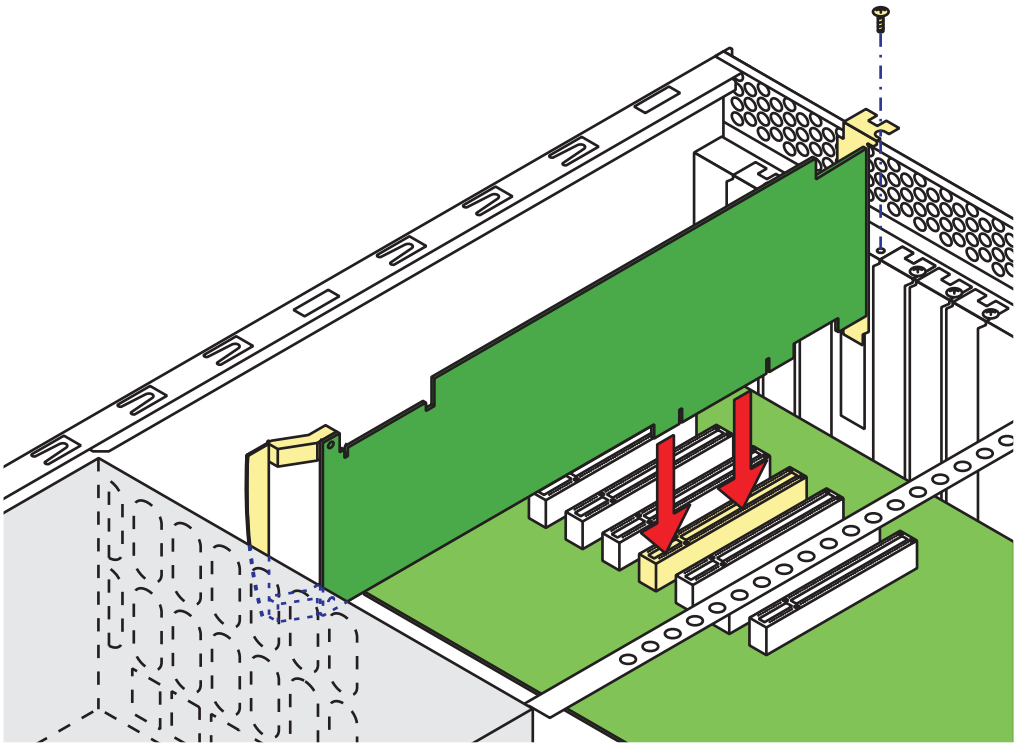
After you verify that the settings are correct, install the MAS port boards:

CAUTION:

Verify that all port boards in an MAS are of the same type. You cannot mix board types within the same MAS, such as analog boards with DSE or QSIG.

1. Slide the slot retainer bracket on the port board into the slot guide on the chassis.
2. Align the edge connector on the port board with the slot connector. Apply pressure to the top of the board only. Push down until the edge connector is firmly seated. See Figure 9.

Figure 9: Installing a port board in a customer-provided MAS



3. Replace and tighten the retaining screw for the port board.
4. Repeat Steps 1 through 3 to install any additional port boards.

5. *If the MAS has multiple port boards,* attach the Computer Telephony (CT) bus cable to connect all the port boards:
   a. Position the CT bus cable so the colored stripe on the ribbon cable faces the ports at the back of the chassis.
   b. Start with the board in the highest numbered slot. Attach the end connector on the bus cable to the CT bus edge connector at the top of the board.
   c. Connect the next bus connector to the next port board, and so on.
   d. If the cable has extra connectors or loose ribbon cable, tuck down the cable so it does not snag when you replace the cover.
6. Replace the chassis cover.
7. Plug in the AC power cord.
8. Restore power to the server.

   The server boots.

Disabling the Dialogic hardware

The Microsoft Windows software automatically detects the Dialogic port boards that you just installed. You configure these boards later as part of the Modular Messaging software installation. Do *not* install the Dialogic drivers at this time.

To temporarily disable the Dialogic port boards:

1. After the server boots, log on using an account that has permission to install software, such as the local administrator.
2. The system runs a **Found New Hardware Wizard** once for each new Dialogic port board installed in the MAS. To complete the wizard:
   a. On the **Welcome** screen, use the default option to **Install the software automatically**. Click **Next**.
   b. Wait while the system searches for a driver.
   c. When the wizard reports that it **Cannot Install this Hardware**, click **Finish**.
3. Repeat Step 2 for each repetition of the Found New Hardware Wizard.

   Note:

   You install the Dialogic drivers later with the rest of the Modular Messaging software.

Connecting MAS port boards to the switch

Connect the MAS port boards to the PBX (switch), as described in this section.

To connect MAS port boards to the switch:

1. Assemble the required cables.

   Note:

   Port boards ordered through Avaya ship with the correct cables.

2. Connect each port on the port boards to the switch (PBX) as required:

   Note:

   Check the numbering on the board faceplate to verify that you are connecting the correct cable to the correct port.

- **For E1-QSIG or T1-QSIG boards:**

  a. Connect the port on the Dialogic E1-QSIG or T1-QSIG board using an RJ-48C Ethernet cable.

  b. The other end of the cable must be connected to the QSIG board on the corporate switching system. The organization responsible for maintaining the corporate switch must make this connection. See the customer contract or the statement of work.

- **For set emulation boards:**

  a. Connect each port on the Dialogic set emulation (DSE) board using the D/82U cable (Intel part number 86-0155-001).

  b. The other end of the cable must be connected to a 4-wire punch-down block on the corporate switching system. The organization responsible for maintaining the corporate switch must make this connection. See the customer contract or the statement of work.

- **For analog boards:**

  a. Connect each port on the installed analog boards to one end of a standard RJ-11 tip/ring cord. You can also use individual tip/ring cables and a 12-port harmonica. Note which cables connect to which ports.

  b. The other end of the cable must be connected to an analog line on the corporate switching system. The organization responsible for maintaining the corporate switch must make this connection. See the customer contract or the statement of work.

Completing the hardware installation

To complete the hardware installation on a customer-provided server:

1. The Dialogic port boards require their own drivers and software for board configuration. You install the Dialogic drivers and software as part of the Modular Messaging software installation. For more information, see Running the Modular Messaging Configuration wizard on page 69.
2. If you intend to access this server remotely using a modem, verify that the modem is correctly installed and configured. For example, a remote support center might need to dial in to this server for troubleshooting or maintenance.
   a. For information about modem installation, setup, and operation, see the documentation provided with the modem.
   b. For information about configuring the Modular Messaging software to use a modem, see Chapter 6: Configuring the voice mail system on page 79.

Appendix E: Updating Modular Messaging software

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 (SP) or Avaya software patches (hotfixes).

Topics in this appendix include:

- Obtaining software updates from the Web on page 303
- Installing software updates on each MAS on page 304

Considerations for applying updates include:

- You can apply multiple hotfixes to a system.
- Modular Messaging components can have multiple updates applied to them.
- If you apply a Service Pack, the program automatically uninstalls all previously applied hotfixes, patches, and Service Packs.

Obtaining software updates from the Web

Obtain the latest Avaya software updates from the Web.

To obtain any Avaya software updates for this system:

1. Use a computer that can access the Internet.
2. Go to the Avaya Support Web site at http://www.avaya.com/support.
3. Download any files needed to update a Release 5.2 system. For example, download the latest Modular Messaging 5.2 Service Pack. Make sure that you download any instructions required to install the Service Pack or software update.
4. Copy the downloaded files to a USB storage device such as a flash drive, memory stick, or equivalent.

   The files are often bundled in a compressed archive, such as a zip file. Use the appropriate tools on your computer to extract the files into an appropriate directory.

Installing software updates on each MAS

To start the update procedure, you must copy the Avaya software updates to each MAS. You then run an installation wizard to install the updates.

Copying files to the MAS

To copy the Avaya software updates to an MAS:

1. Switch the monitor to show the appropriate MAS.
2. Insert the USB drive into any USB port on the server.
   - You can use any of the available USB ports on the back of the server.
   - Remove the front bezel to access the USB port on the front of an Avaya S3500-family message server.
3. Copy the software update files to the MAS:
   a. Navigate to the appropriate directory on the USB storage device.
   b. Right-click the software update file that you downloaded in Obtaining software updates from the Web on page 303. For example, file *MAS520100.exe*. Select **Copy**.
   c. Navigate to the ***C:\Avaya_Support directory***.
   d. Right-click in a blank area in the right pane, and select **Paste**.
   e. Verify that the correct file is listed in the ***C:\Avaya_Support directory***.
   f. If you downloaded more than one file, repeat Steps b through e to copy all the software files and the update instructions to the MAS.
4. Safely remove the USB drive from the server:
   a. Double-click the icon on the task bar to **Safely Remove Hardware**.
   b. Follow the prompts to safely remove the USB drive.
5. Repeat Steps 1 through 4 for each MAS in the system.
6. Open and review the installation instructions for this specific software update.

Installing the updates on each MAS

Important:

Always read the Release Notes that come with each software update. The following are general instructions for installing updates on each MAS. The Release Notes provide specific software update information.

To install the Avaya software updates on this MAS:

1. Double-click the software update file.

   The program unpacks the file, and then runs the Modular Messaging Installation wizard.

2. In the Modular Messaging Installation Wizard window:

   a. Verify that all applicable patches for this system are selected.

   b. Click **Install**.

   If the **Install** button is not active, you do not need to apply these software updates to the system. Continue with Step 6.

   Note:

   For installation procedures and a description of components that can be installed, click the **Help** button on the installation wizard window.

3. If you are installing a Service Pack (SP), an **Installation Wizard - Update Warning** window opens. The window displays the hotfixes and Service Packs that the program must uninstall before the update can proceed. Click **Continue**.

   Note:

   If hotfixes are applied to the system that are not included in the SP update, the program lists them with a warning.

4. If this system does not have the correct version of Windows Installer, install it now. Otherwise, continue with Step 5:

   a. The **Open File - Security Warning** window prompts you to install a WindowsInstaller application from Microsoft Corporation. Click **Run**.

   b. Follow any additional prompts to install the new Windows Installer application. If the program prompts you to restart the server, restart the system.

   c. If the new version of Windows Installer fails to install, install the updated WindowsInstaller application before you proceed. For example, you might need to download the application separately, and install it using the local administrator account for this MAS.

5. After you click **Install**, monitor the software update progress:

   a. In the **Services** window, the wizard stops all appropriate Modular Messaging and related services.

b. Windows Installer installs all relevant software updates on the MAS.

c. In the **Services** window, click **Continue with installation**. You do not have to wait for all services to restart.

d. After the installation is complete, click **Close**.

6. To verify the software updates that are installed on this MAS:

a. Log on to the MAS.

b. Select **Start > Programs > Avaya Modular Messaging.**

c. Click **About Modular Messaging** and verify the version of MM installed.

d. Click **Patches** and verify that service packs and patches are installed.

7. After installation and verification is complete, close all open windows.

Appendix F: Configuring and testing port boards

Overview

This appendix describes how to configure and test Dialogic port boards. Dialogic port boards are installed in some MASs, depending on the switch integration.

Note:

An MAS that uses an IP H.323 or IP SIP switch integration has no port boards. You do all configuration for these switch integrations using the Voice Mail System Configuration (VMSC) program. For more information, see Configuring port boards and switch integration on page 100.

CAUTION:

Modular Messaging Release 5.2 does not support Dialogic port boards with new Installations and migrations on Avaya-provided hardware or customer-provided hardware.

This section contains the following topics:

- When to configure port boards on page 307
- Configuring port boards on page 309
- Testing the port boards on page 317

When to configure port boards

In Release 5.2, you must configure Dialogic port boards only if:

- Dialogic port boards are installed in this MAS *and*
- The Avaya Modular Messaging Configuration Wizard does not automatically configure the Dialogic port boards.

Note:

S8800 1U server does not support Dialogic port boards.

The Avaya Modular Messaging Configuration Wizard automatically configures any installed Dialogic port boards for several switch integrations, including:

- Avaya (QSIG)
- Cisco (QSIG)
- Nortel NT M-1 (QSIG)

- Siemens Hipath (QSIG)

To verify if a particular switch integration supports automatic configuration of the Dialogic port boards, open the Data Collection Tool (DCT) executable file.

1. On the MAS, navigate to the directory
   C:\Program Files\Avaya Modular Messaging\Install\MISCM
2. Double-click the executable file (**MMDCT.exe**) to open the Data Collection Tool.
3. Click the **Switch integration method** screen to see the list of supported switch integrations.
4. Close the DCT executable file and close all open windows.

Supported port boards

The number and type of supported port boards varies, depending on the hardware used and the release during which the port boards were installed.

Important:
S8800 1U server supports only SIP and does not support any port boards. An MAS running on an S8800 hardware supports a maximum of 96 ports.

- Systems with Avaya MASs that were upgraded from an earlier release might use either customer-provided servers, S8730 servers or S3500 servers. Upgraded MASs can have a varying number of port boards installed. The number of port boards depends on the original software release when the boards were installed, and the number of TUIs in use. Table 17 lists supported Dialogic port boards for customer-provided and S8730 servers.

Table 17: Supported Dialogic port boards: S8730 server and CPE hardware

Protocol	Maximum Ports per MAS	Supported port boards	Maximum cards per MAS	Dialogic files on documentation library
Analog	36 12	Dialogic D/120JCT-LS-EW 12-port board Dialogic D/41JCT-LS-EW 4-port board	3 3[2]	**D/120JCT-LS** (PDF) **D/41JCT-LS** (PDF)
Digital Set Emulation	24 8	Dialogic D/82JCT-EW	3	**D/82JCT-U PCI Univ** (PDF) **D/82JCT-U** (PDF) *Supported for upgrades only. customer-provided servers support up to 6.*

Table 17: Supported Dialogic port boards: S8730 server and CPE hardware (continued)

Protocol	Maximum Ports per MAS	Supported port boards	Maximum cards per MAS	Dialogic files on documentation library
E1-QSIG	88 29	Dialogic D/ 600JCT-1E1-120-EW	3	**D/600JCT-1E1** or **D/600JCT-2E1** (PDF) **D/300JCT-E1** (PDF) *Supported for CPE upgrades only.*
T1-QSIG	69 23	Dialogic D/480JCT-1T1 -EW	3	**D/480JCT-1T1** (PDF) **D/240JCT-T1** (PDF) *Supported for CPE upgrades only.*
H.323 integration	30	None	None	None
SIP/RTP **SIP/SRTP**[1]	96 96	None	None	None

1. SIP and H.323 transmit voice as IP packets over the LAN cards. Therefore, does not need separate port boards.

- New Release 5.2 systems can use the following hardware:
  - Avaya-provided MASs always use S8800 1U server hardware. All S8730 servers or S3500 servers support a maximum of two port boards each.
  - New installation of Modular Messaging Release 5.2 that use a customer-provided server do not support dialogic port boards. For previous releases, the number of port boards depend on the board type and the number of PCI slots available in the customer-provided server. For more information about customer-provided servers, see Table 6: Supported MAS port boards for customer-provided servers on page 286.

The Dialogic documents provide details about installing and connecting the port boards. The documents are available on the *Avaya Modular Messaging Documentation* library on Avaya Support Web site at http://www.avaya.com/support. For instructions on obtaining Avaya documents, see Downloading user documentation on page 5. For the latest version of the Dialogic guides, see the Quick Install Cards Search Tool on the Intel Telecom Boards Web site.

Configuring port boards

Manual port board configuration involves three phases:

1. The appropriate party must administer the switch for the port boards using the configuration notes for this particular switch (PBX) integration. For instructions on obtaining the most recent configuration notes, see Downloading configuration notes on page 4.

CAUTION:

You can install this system only by using the required configuration notes for this switch or PBX. The PBX administrator *must* have administered the ports on the switch before you can proceed.

2. Configure and test the port boards as described in this section. Some steps require you to use the configuration notes.
3. Complete the port board configuration as described in Chapter 6: Configuring the voice mail system on page 79.

Continue based on the type of port boards installed in this MAS:

- Configuring T1-QSIG or E1-QSIG boards on page 310
- Configuring set emulation boards on page 312
- Configuring analog port boards on page 314

CAUTION:

If the window displays no port boards when you run the Dialogic Configuration Manager, you might need to reseat or replace some of the boards. For more information, see the appropriate maintenance information for this Modular Messaging system on the documentation library:

- For S8730 servers, see *Avaya Modular Messaging S8730-Family Hardware Maintenance and Additions*
- For S3500 servers, see *Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions*

For information on placing and numbering the Dialogic port boards, see *Avaya Modular Messaging S8730-Family Hardware Maintenance and Additions* guide and *Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions* guide.

Configuring T1-QSIG or E1-QSIG boards

Any of the following QSIG port boards might be installed in an MAS:

- Dialogic D/480JCT-1T1 board
- Dialogic D/480JCT-1T1- EW
- Dialogic D/600JCT-1E1
- Dialogic D/600JCT-2E1
- Dialogic D/600JCT-1E1- 120- EW

Note:

Avaya supports the D/240JCT-T1 and D/300JCT-E1 QSIG boards *only* for CPE upgrades from Release 1. Avaya-provided servers do *not* support these boards

The maximum number of port boards per MAS varies, depending on the server hardware. For more information, see Supported port boards on page 308.

To configure QSIG boards:

1. Click **Start > Programs > Intel Dialogic System Release > Configuration Manager - DCM**.

   The **Intel Dialogic product Configuration Manager** window opens.

2. If a popup window opens, connect to the MAS as follows:

   a. In the **Computer Name** window, verify that **Local** is selected and that the correct server name is shown, such as *MYMAS1*.

   b. Click **Connect**.

   Note:

   The system displays this window only the first time that you access the Dialogic Configuration Manager application.

   The Dialogic software locates any installed port boards.

3. Verify that all Dialogic services are stopped. All boards should show a red icon.

   Note:

   If the board icon shows an X, the board is disabled. To enable it, right-click the board and select **Enable device(s)**.

4. Under Configured Devices, double-click the name of the first Dialogic board, such as *#0*.

5. In the **Intel Dialogic product Configuration Manager - Properties** window:

   a. Click the **Interface** tab and select the **ISDNProtocol** parameter.

   b. Select the correct value for this board from the pull-down list:

   - For E1-QSIG: select **QTE**
   - For T1-QSIG: select **QTU**

   c. Click the **Telephony Bus** tab and select the **PCMEncoding** parameter.

   d. Select the correct value for the installed board from the pull-down list:

   - For E1-QSIG: select **A-Law** for most countries, particularly Europe
   - For T1-QSIG: select **μ-Law** (mu-Law) for the United States and Japan

   e. Click the **Misc** tab. For the **FirmwareFile** parameter, verify that the value is **default**.

   f. On the **Misc** tab for the **FirmwareFile2** parameter, verify that the value is **spfax.fwl.** This parameter will only appear for the D480JCT-1T1, D/600JCT-1E1 or D/600JCT-2E1 dual span QSIG boards.

   g. Click the **Country** tab and select the **Country** parameter.

   h. On the pull-down list of values, always use **United States** for either type of board.

i. Click **OK** to close the properties window.

6. Repeat Steps 4 and 5 for any other installed Dialogic boards, such as *#1*.
7. After all boards are configured, click the green **Start** button on the button bar.

   Wait for service to start. When service is started, the **Stop** button becomes active and the installed boards show a green light.
8. Verify that the port boards are operating correctly.
   a. Check the LED display on the Dialogic board faceplate.
      - A red status LED lights on the back of the port board during driver startup.
      - If the drivers start successfully, the board whose port is connected to the PBX shows a green LED within 30 seconds. LEDs on the other boards remain red.

   b. If a problem occurs, check the board configuration, the physical connections between the board and the PBX, or the PBX configuration. Repeat Steps 4 through 8 as needed.
9. Close the **Intel Dialogic product Configuration Manager** window.
10. Continue with Testing the port boards on page 317.

Configuring set emulation boards

An MAS supports 8-port Dialogic Digital Set Emulation (DSE) boards. The maximum number of port boards per MAS varies, depending on the server hardware. For more information, see Supported port boards on page 308.

Note:

Avaya supports the non-universal D/82JCT-U board for upgrades only.

To configure digital set emulation boards:

1. Click **Start** > **Programs** > **Intel Dialogic System Release** > **Configuration Manager - DCM**.

   The **Intel Dialogic product Configuration Manager** window opens.
2. If a popup window opens, connect to the MAS as follows:
   a. In the **Computer Name** window, verify that **Local** is selected and that the correct server name is shown, such as *MYMAS1*.
   b. Click **Connect**.

   Note:

   The system displays this window only the first time that you access the Dialogic Configuration Manager application.

   The Dialogic software locates any installed port boards.
3. Verify that all Dialogic services are stopped. All boards should show a red icon.

Note:

If the board icon shows an X, the board is disabled. To enable it, right-click the board and select **Enable device(s)**.

4. Under Configured Devices, double-click the name of the first Dialogic board, such as *#0*.
5. In the **Intel Dialogic product Configuration Manager - Properties** window:
   a. Click the **Telephony Bus** tab and select the **PCMEncoding** parameter.
   b. On the pull-down list of values, select either **A-Law** or μ**-Law**, depending on your location. Usually, **A-Law** is Europe and μ**-Law** (mu-Law) is United States and Japan.
   c. Click the **Misc** tab.
      1. Select the **FirmwareFile** parameter. In the **Value** field, select or type **D82U.fwl**. The **Value** field is editable.
      2. Select the **PBXSwitch** parameter. On the pull-down list of values, select the name of the PBX. For example, use *Lucent 2-wire* for an Avaya G3 switch.

   Note:

   For a Siemens Hicom 300/9006 PBX, select Siemens Rolm 9006.

   d. Click the **Country** tab and select the **Country** parameter. On the pull-down list of values, select the country.
   e. Click **OK** to close the properties window.
6. Repeat Steps 4 and 5 for any other installed Dialogic boards, such as *#1*.

CAUTION:

If the DSE boards are connected to a Nortel (NTM-1) PBX, you must restart the MAS before you start the Dialogic drivers. Close the DCM and restart the system now. When the restart is complete, log back in and reopen the DCM as in Step 1, and then continue with Step 7.

7. After all boards are configured, click the green **Start** button on the button bar.

   Wait for service to start. When service is started, the **Stop** button becomes active and the installed boards show a green light.
8. Verify that the port boards are operating correctly.
   a. Check the LED display on the Dialogic board faceplate. Verify the code for each port:
      - Ports that are connected to a telephone line and functioning correctly show 0 and the port number, such as *00* or *01*.
      - Ports that are not connected to a telephone line or not functioning correctly show *En*, where *n* is the port number. For example, the display reads *E3* if port 3 has an error.
   b. If the system displays any *En* error, check the board configuration, the physical connections between the board and the PBX, or the PBX configuration. For example, verify that you configured the correct PBX. Repeat Steps 4 through 8 as needed.

9. Close the **Dialogic product Configuration Manager** window.
10. Continue with Testing the port boards on page 317.

Configuring analog port boards

The following analog port boards might be installed in an MAS:

- Dialogic D/41JCT-LS 4-port Tip/Ring
- Dialogic D/41JCT-LS- EW 4-port
- Dialogic D/120JCT-LS 12-port Tip/Ring board
- Dialogic D/120JCT-LS- EW 12-port

The maximum number of port boards per MAS varies, depending on the server hardware. For more information, see Supported port boards on page 308.

To configure any of these analog boards:

1. Click **Start** > **Programs** > **Intel Dialogic System Release** > **Configuration Manager - DCM**.

   The **Intel Dialogic product Configuration Manager** window opens.

2. If a popup window opens, connect to the MAS as follows:

   a. In the **Computer Name** window, verify that **Local** is selected and that the correct server name is shown, such as *MYMAS1*.

   b. Click **Connect**.

   Note:

   The system displays this window only the first time that you access the Dialogic Configuration Manager application.

   The Dialogic software locates any installed port boards.

3. Verify that all Dialogic services are stopped. All boards should show a red icon.

   Note:

   If the board icon shows an X, the board is disabled. To enable it, right-click the board and select **Enable device(s)**.

4. *For a D/120JCT-LS board:* You must load the new firmware separately in Release 5.2, or the 12-port boards will not work correctly. For example, fax service will not work.

   Note:

   The D/41JCT-LS board uses the default.fwl file and does not need to be set. If this server uses 4-port analog boards, continue with Step 6.

   To load the new firmware for a 12-port analog board in Release 5.2:

   a. Under Configured Devices, double-click the name of the Dialogic board, such as *#0*.

   b. In the **Intel Dialogic product Configuration Manager - Properties** window, click the **Misc** tab.

      1. Click the **FirmwareFile** parameter. In the value field, select or type **spfax.fwl**.
      2. Click **OK** to close the window.

   c. Repeat Steps a and b for any other installed Dialogic boards, such as *#1*.

   CAUTION:

   Make no other property changes at this time.

5. Reload firmware:

   a. After you set the firmware parameter on all installed boards, close the **Intel Dialogic Product Configuration Manager** window.

   b. Wait 30 seconds for all the Dialogic processes to completely stop.

   c. Reopen the Intel Dialogic product Configuration Manager application to load the new firmware file. For more information, see Step 1.

   d. Click the green **Start** button on the button bar.

   e. Wait for the device to start. When service is started, the **Stop** button becomes active and the installed boards show a green light.

   Note:

   If the drivers fail to start, complete Steps 6 through 11. You must then completely power down and power up the MAS. After the server boots, continue with Testing the port boards on page 317.

   f. Click the **Stop** button to stop the Dialogic drivers.

   g. After all boards show a red icon, continue with Step 6.

6. Under Configured Devices, double-click the name of the first Dialogic board, such as *#0*.

   CAUTION:

   If you cannot find a suitable TSF file for this PBX, you must build an appropriate tone file now or the integration will not work. Click **Cancel** in this window, and see Appendix C: Creating a new tone file on page 277.

7. In the **Intel Dialogic product Configuration Manager - Properties** window:

a. Click the **Files** tab.

b. Select the **TSFFileName** parameter, if it is not already selected.

Note:

For a D/41JCT-LS board, you must highlight the **Configured Devices** parameter on the DCM display when you select **Configure Device**. You can then view the **TSFFileName** parameter.

c. Locate the prerecorded TSF file for this PBX or switch:

1. Click the**...** button to browse. In the **Look in** field, navigate to the ***C:\Avaya_Support\Tone_Files directory***.
2. In the **Search File** window, select a TSF file that is appropriate for the PBX to which you are connecting, such as *Avaya-G3-US.tsf*. Double-click the file name.

The system displays the appropriate TSF file in the **Value** field.

Note:

You can type in the **Value** field. This field is editable.

8. After an appropriate TSF file is selected, click the **Misc** tab.

a. Click the **TSFFileSupport** parameter.

CAUTION:

You must have selected an appropriate TSF file for this PBX *before* you set the TSFFileSupport value to **Yes**, or errors might occur.

b. From the **Value** drop-down list, select **Yes**.

c. Click the **DisconnectTone** parameter. From the **Value** drop-down list, select **Yes**.

d. Click **OK** to close the window.

9. Repeat Steps 6 through 8 for any other installed Dialogic boards, such as *#1*. Verify that the settings are correct, and set any values if needed.

10. After all boards are configured, click the green **Start** button on the button bar.

Wait for service to start. When service is started, the **Stop** button becomes active and the installed boards show a green light.

Note:

For a D/120JCT-LS board: If the drivers failed to start in Step 4, you must completely power down and power up the MAS. After the server boots, continue with Testing the port boards on page 317.

11. Close the **Intel Dialogic product Configuration Manager** window.

12. Continue with Testing the port boards on page 317.

Testing the port boards

Test all port boards and channels to verify that they can send and receive calls.

Note:

Sometimes after you apply settings to a port board, the board comes up in a bad state. The Dialogic drivers consistently fail to start, and the Event Viewer shows **dlgc_log** errors. If this problem occurs, take the power off the boards. Turn off the server, and then turn on the server again. The power cycle corrects the port board problems.

Preparing for the test

Prepare for port board testing as follows:

1. Stop Modular Messaging voice service:
   a. Access the window to monitor services using one of these methods:
      - Double-click the **Monitor** icon on the desktop. In the left pane, click **Services**.
      - Right-click **My Computer** and select **Manage**. In the **Computer Management** window, in the left (Tree) pane, expand **Services and Applications**, and click **Services**.
   b. In the right pane, scroll down to **MM Messaging Application Server**.
   c. Right-click **MM Messaging Application Server** and select **Stop**.
2. *For software-only upgrades,* the Dialogic Line Tester program is not yet installed. Access the test program on the application media as follows:
   a. Insert Disk 1 of the *Avaya Modular Messaging Messaging Application Server Software* media into the MAS drive. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
   b. Close the drive door and wait for the green LED to go out. Click **OK**.
   c. Navigate to the MAS drive.
   d. Navigate to the **Install** directory, and then to the **DLTest** subdirectory.
   e. Double-click the file **DLTest.exe**.

   The **Dialogic Line Test Application** window opens.
3. *For T1-QSIG or E1-QSIG boards,* set up the test options as follows:
   a. Click **Start** > **Programs** > **Avaya Modular Messaging** > **Dialogic Line Tester**.
   b. In the **Dialogic Line Test Application** window, click **Tools** > **Options**.

c. In the **Options** window, select the correct values for each field. Use the configuration notes to identify the correct values:
   - For **Layer 1 Protocol**, select the required ISDN protocol from the drop-down list.
   - For **Number Type**, select the destination number type.
   - For **Number Plan**, select the destination number plan.

Note:

The values you select here must be the same as those entered on the PBX or switch. Check the configuration notes.

d. After you select the correct values, click **OK**.

Testing the ports

To test Dialogic port board functionality:

1. Access the Dialogic Line Test application using one of these methods:
   - Click **Start** > **Programs** > **Avaya Modular Messaging** > **Dialogic Line Tester**.
   - *For software-only upgrades,* access the Dialogic Line Tester program from the applications media. For this procedure, see Step 2 in Preparing for the test on page 317.

   The **Dialogic QSIG - Line Test Application (or DLTest)** window opens. The name of the window varies, depending on the type of port boards installed.
2. Verify that all port numbers and channel designations are listed.
3. Test the incoming call connectivity of all ports as follows:
   a. From a handset on the same PBX, dial each port individually.
      - For QSIG boards, repeatedly dial the number for that group of ports. The switch connects to the next port in the list for each new call.
      - For analog and set emulation boards, use the individual port extensions.
   b. Check the **Status** column.
      - Verify that each port shows **Received call** followed by **Connected**.
      - For different status conditions, see Status messages for Dialogic Line Test on page 319.

      The system should answer each connected call with a standard welcome message.

Table 18: Status messages for Dialogic Line Test

Status	Description	Highlight
Channel starting…	The channel is being started.	Normal
Channels idle…	The channel is idle.	Normal
Waiting for call…	The channel is waiting for an incoming call.	Normal
Received call…	An incoming call is being processed.	Normal
Dialling number…	A number is being dialed to make an outgoing call.	Normal
Resetting…	The user reset the channel.	Normal
Line Busy.	An outgoing call was made, but a busy tone was detected.	Normal
No Answer.	An outgoing call was made, but the call was not answered.	Normal
Connected.	An incoming or outgoing call was answered, so the call is now connected.	Normal
Call was disconnected.	An incoming or outgoing call was disconnected.	Normal
Error.	A general error with the channel occurred.	Error
Error, No Dial tone detected.	An outgoing call was made, but no dial tone was detected before dialing.	Error

4. Test the outcalling capability of all ports.
   a. Select a port in the **Dialogic Line Test Application** window under **Port Number**.
   b. Type the number of an extension on this PBX in the **Dial Number** field and click **Dial Number**.
   c. When the dialed extension rings, answer the call and hang up.
   d. Select the next port number, and click **Dial Number** again.
   e. Repeat Steps c and d until all ports are tested.
5. After testing is complete, close the **Dialogic Line Test Application** window.
6. If a problem occurs, check:
   - the board configuration
   - the physical connections between the board and the PBX
   - the PBX configuration itself

   For example, verify that you have configured the correct PBX type and administered the values according to the current configuration notes.
7. Continue with Chapter 6: Configuring the voice mail system on page 79.

Appendix G: Reloading software on an Avaya MAS

This appendix describes how to reload the operating system and application software on an Avaya Messaging Application Server (Avaya MAS) or an Avaya-provided supplementary server. You might install new software after a hard disk is replaced or as part of the upgrade of an Avaya MAS.

Loading new MAS software

To copy new software to the Avaya Messaging Application Server (Avaya MAS) or Avaya-provided supplementary server:

1. If the server is not on, turn on the server.
2. Verify that the monitor is showing the correct server.
   - For a 2-port Belkin KVM switch, the MAS is connected to one of the two computer ports.
   - For an 8-port Belkin KVM switch, the first MAS port is labeled **VGA 02**. Subsequent MASs and any supplementary servers, if present, are connected to computer ports **VGA 03**, **VGA 04**, and so on.
3. If the monitor displays a different server, toggle the ports to show the correct server.
   - To have a 2-port Belkin KVM switch show a different server:
     a. Slowly press **Scroll Lock** twice.

        The LED on top of the Belkin KVM switch starts to blink.

     b. Type the port number on the keyboard. For example, type **2** for port 2.
   - To have an 8-port Belkin KVM switch show a different server:
     a. Slowly press **Scroll Lock** twice within 2 seconds.
     b. Select the server to display using one of these methods:
        - Press the up (or down) arrow key to change to the server connected to a higher (or lower) port number.
        - Type the port number on the keyboard. For example, type **2** for port 2.

     For complete user and troubleshooting instructions, see the KVM switch documentation.

Loading the new software

To load the new software:

1. Insert the *Avaya Modular Messaging Messaging Application Server (MAS) and Boot Software for Microsoft Exchange and IBM Domino* media into the DVD drive. Make sure you are inserting the MM MAS Image DVD specified for the hardware you are using. Wait for the green LED on the drive to go out.
2. Press **Ctrl**+**Alt**+**Del** to restart the system.
   a. In the Windows Security window, click **Shut Down...**
   b. In the Shut Down Windows window, select **Restart**. Click **OK**.
3. When the computer starts to boot, the system might display a warning that the hard drive contents will be overwritten.
   a. Press any key to continue.

      A message confirms that the hard drive will be overwritten.

   b. Press any key to continue.

   The MAS starts to copy the disk image to the hard disk. The entire copy procedure takes up to 30 minutes.
4. At the prompts, insert the disk. When the DVD drive light turns dark, click **OK**.
5. When prompted, remove the media before the system restarts. Press any key to continue.

   The system restarts and runs the Windows Setup program.
6. If a modem is connected, a **Hardware Installation** window opens. Click **Yes** to continue the installation.
7. The **Windows Setup** wizard runs. To complete the wizard:
   a. On the **Welcome** screen, click **Next**.
   b. On the **License Agreement** screen, choose **I accept this agreement**. Click **Next**.
   c. On the **Your Product Key** screen, type the Windows product key for this server.

   Note:

   Each Windows computer has a unique product key for Windows 2003 or Windows 2003 R2. Enter the number exactly as shown.

   - On an S8800 1U server, the product key sticker is located on top of the server chassis.
   - For an S8730 server, the product key sticker is located on the right-hand edge of the server chassis.

- For an S3500 server, the product key sticker is located inside the empty drive tray on the lower-left of the server chassis. You can remove the drive tray to easily read the sticker.

d. Click **Next**.

The server automatically restarts.

Preparing the server to boot

You must load all required information and activate the operating system before you proceed with server configuration:

1. When the system prompts you to log on:
   a. Press **Ctrl**+**Alt**+**Del**.
   b. In the **Log On to Windows** window, leave the user name as **Administrator**.
   c. Leave the password field blank.
   d. Press **Enter** or click **OK**.

   CAUTION:
   If you are completing an upgrade or recovery that requires a DCT file, you must copy the latest DCT data file to the **C:** directory now. Some servers do not recognize a USB drive after a system restart.
2. Activate the Microsoft Windows operating system before you restart the server. Use site-specific procedures. For more information, see Activating Microsoft Windows on page 324.
3. After the Microsoft Windows operating system is active, double-click the **MM_Setup** icon on the desktop.

   An **MM_Setup** window opens.
   a. At the prompt, insert the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1) and press any key to continue. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
   b. Follow the instructions that appear.
   c. When the system prompts you, remove the DVD from the MAS and press any key to continue.

      MM_Setup reports that Modular Messaging configuration program will run after the server restarts.
   d. Press any key to continue.

   The computer stores the information and shuts down.
4. To bring the MAS into service, continue with the appropriate procedure:

- For an Avaya MAS upgrade, see Running the Modular Messaging Configuration Wizard on page 177.
- For an Avaya MAS disk failure recovery, see Appendix I: Catastrophic Disk failure recovery on page 329.

Activating Microsoft Windows

You must activate the Microsoft Windows operating system whenever you reload the operating system. You must activate the Windows operating system before you run MM_Setup.

The Microsoft Windows activation procedure requires you to use either the Internet or, if the customer site does not have an Internet connection, a telephone.

- For telephone activation, continue with Activating Microsoft Windows using a telephone on page 324.
- For Internet activation, continue with Activating Microsoft Windows through the Internet on page 325.

Activating Microsoft Windows using a telephone

To activate the Microsoft Windows operating system using a telephone:

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**.

   The program generates a new installation ID.
3. On the **Activate Windows by Phone** screen:
   a. Select the country in which this Modular Messaging system is installed.
   b. Call the appropriate telephone number shown on the screen.
   c. Follow the voice prompts or the directions from the customer service representative to provide the unique installation ID shown on the screen.
   d. Enter the confirmation ID that the automated system or customer service representative gives you.
   e. Click **Next**.
4. On the confirmation screen, click **Finish**.
5. Return to Preparing the server to boot on page 323, Step 3.

Activating Microsoft Windows through the Internet

To activate the Microsoft Windows operating system through the Internet:

1. Double-click the **Internet Explorer** icon on the desktop.
2. At the Enhanced Security message, click **OK**.
3. In Internet Explorer, click **Tools** > **Internet Options**.
   a. In the **Internet Options** window, click the **Connections** tab.
   b. Click **LAN Settings**.
   c. In the **Local Area Connection (LAN) Settings** window, specify the settings to use for this site. Click **OK**.
   d. Click **OK** to close the **Internet Options** window.
   e. Close Internet Explorer.
4. Click **Start** > **Activate Windows**.
5. In the **Activate Windows** window:
   a. Click **Yes, let's activate Windows over the Internet now**.
   b. Click **Next**.
   c. When the system prompts you to register the system, click **No**.

   The program checks for Internet connectivity.
6. If connectivity fails, set up or adjust the Internet connections. Complete the screen and click **Next**.
7. On the **Thank you** screen, click **OK**.
8. Return to Preparing the server to boot on page 323, Step 3.

Appendix H: Removing Modular Messaging components from an MAS

This appendix describes how to remove Modular Messaging software components from a server where they are currently installed. Normally this procedure is used to prepare a server for reassignment to another purpose.

CAUTION:

Do not uninstall any of the following Modular Messaging services from an MAS that is running the Messaging Application Server service.

To stop running unneeded services on an in-service MAS, move services to other servers using the Modular Messaging administration tools and disable the services that the server does not need.

- MM Alarming Server service
- MM Audit Service
- MM Call Me
- MM Event Monitor Server
- MM Fault Monitor Service
- MM Fax Service
- MM Mailbox Monitor
- MM Messaging Application Server
- MM MWI
- MM Performance Monitor Server
- MM Process Monitor Server
- MM Service Connector
- MM Tracing Server

Removing software components

To remove Modular Messaging software components, use the Modular Messaging Uninstallation Wizard.

1. Click **Start** > **Settings** > **Control Panel**.
2. From the Control Panel window, double-click **Add/Remove Programs**.
3. In the **Add/Remove Programs** window, scroll down the list of currently installed programs to **MM Uninstallation Wizard**.

   Important:
   Do not use **Add/Remove Programs** to uninstall the **MM** services listed. Use only the **MM Uninstallation Wizard**.
4. Select the Modular Messaging software components that you want to remove.
5. Click **Uninstall** and follow the prompts to confirm your choices.
6. The removed components will continue to appear in the **Add/Remove Programs** list until you close and reopen **Add/Remove Programs**.

Appendix I: Catastrophic Disk failure recovery

This appendix describes the procedure for recovering from a catastrophic disk failure on a system that is running Modular Messaging Release 5.2 software. See the checklist that is appropriate for your MAS:

- For an Avaya MAS, see Recovering from a catastrophic disk failure on an Avaya MAS on page 330.
- For a customer-provided MAS, see Recovering from a catastrophic disk failure on a customer-provided MAS on page 336.

Recovering from a catastrophic disk failure on an Avaya MAS

An S8730 server or an S8800 server consists of two primary hard disks and the disks are hot swappable. An MAS running on an S8730 server or S8800 server does not fail if one of the hard disks fails. If a hard disk fails, the MAS continues to function and an alarm goes off asking for a replacement of the failed drive. For more information on replacing a hard drive in an S8730 server or S8800 server, see the *Maintaining the Avaya S8730 server for Modular Messaging* guide or *Installing the Avaya S8800 Server for Modular Messaging*.

However, in the rare event of failure of both the disks, the MAS running on the server also fails. In this case, the MAS needs to be rebuilt following the below mentioned procedures.

Overview

In summary, to restore an Avaya MAS you need to:

1. Replace the failed drive
2. Install a new Avaya boot image
3. Perform Windows Product Activation (WPA)
4. Run the Modular Messaging setup utility
5. Run the Modular Messaging Configuration wizard
6. Administer antivirus software
7. Install Modular Messaging Active Directory Exchange extensions
8. Restore customer data
9. Configure the voice mail system
10. Configure services
11. Perform acceptance tests on the entire system
12. Back up the restored system and hand it off to the customer

Table 19: Avaya MAS restore procedure on page 332 lists the steps necessary to restore an Avaya MAS. It contains page references to detailed instructions for each step.

Requirements for restore of Avaya MAS

To successfully restore a system to Modular Messaging Release 5.2, you need:

- A replacement hard disk drive.
- Release 5.2 of the Modular Messaging application software.
  - Avaya Modular Messaging 5.2, MAS for Microsoft® Exchange® & IBM Domino®, Boot Disk for recovery of existing image only.
  - Avaya Modular Messaging Messaging Application Server Software media. For a system with an Exchange 2010 peer mail server, you must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".
  - *Avaya Modular Messaging Documentation*
- The following information and software from the Avaya Support Web site at http://www.avaya.com/support. For more information about how to access these items on the Web site, see Obtaining the DCT data file on page 3.
  - The most current copy of the configuration notes for this switch integration.
  - Avaya software updates that are required to bring the Avaya Modular Messaging software up to date after a restore. Download this software to a USB storage device. For more information about downloading the updates, see Appendix E: Updating Modular Messaging software on page 303.
  - The latest copy of the DCT executable file (**MMDCT.exe**). Download the file from the Avaya support Web site to a USB storage device.
- Customer-provided Microsoft Exchange System Management Tools. (Microsoft Exchange 2003 System Management Tools are highly recommended. The procedures in this chapter describe installation with the 2003 tools.) When installing a system with Exchange 2007 mail servers, you will require the 32-bit version of the Exchange 2007 Management Tools and additional software downloads. For more information, see Installing third-party software for Exchange 2010 on page 52, and Installing third-party software for Exchange 2007 on page 52.
- Microsoft Exchange 2003 Service Pack 2 for Exchange 2003 System Management Tools.
- Access to the most recent backup DCT data file as well as any backup files that will need to be restored to the system.

To restore an MAS configuration after a catastrophic disk failure, you must have a previously saved and updated DCT data file. For information about maintaining a current DCT data file, see Using the DCT to collect information from an MAS on page 130 or see the Data Collection Tool Online Help or its printed version, *Avaya Modular Messaging Data Collection Tool Help*, for a complete description of the procedure to analyze a system with the DCT executable file.

CAUTION:

You cannot restore the MAS without a DCT data file that was created by analyzing the system.

Include the updated DCT data file in any regular, scheduled backups administered for this site so that the file is available if needed for a restore.

Restoring the Avaya MAS

To restore the MAS, complete the tasks in the following checklist. As you complete a task, make a check mark in the " ✔ "column. For additional information or detailed procedures, see the referenced page number.

Table 19: Avaya MAS restore procedure

✔	Procedure	Page	Comments
	Download required Avaya software updates. This includes the latest DCT executable file (**MMDCT.exe**).	4	Web access required.
	Collect any software media that is needed, such as Microsoft Windows updates or antivirus software.	125	Leave customer media on-site.
	For a system with an Exchange 2003 peer mail server, obtain the Exchange System Management Tools and Exchange 2003 Service Pack 2 from the customer. For a system with an Exchange 2007 peer mail server, download Management Tools and additional required software including MAPI Client, Powershell 1.0, Microsoft Management Console 3.0 and .NET 2.0 as needed. For a system with an Exchange 2010 peer mail server, obtain the MAPI Client, PowerShell 2.0, and all additional required software.	46	
	Obtain and review the configuration notes for any changes.	4	Web access required.
	Replace the hard drive. (For instructions on replacing an S3500, S8730, or S8800 server hard drive, see the *Installing the Avaya S8800 Server for Modular Messaging* guide or *Maintaining the Avaya S8730 Server for Modular Messaging* guide or *Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions guide*.)		
	Copy the backup DCT data file (*.mmdct) to a USB storage device with the latest DCT executable file (**MMDCT.exe**).	172	

Table 19: Avaya MAS restore procedure

✔	Procedure	Page	Comments
	Verify that all additional backup files that must be restored are at a location accessible to the MAS, including: • customized tone files • customized prompt files • caller applications • Avaya license files. • SIP certificate files • WSO system services data file • Audit database • Operation history and transaction databases	119	See Backing up the system on page 119, for a complete list of the file names and their locations on the system.
	Switch the monitor to display the Avaya MAS that you are restoring.	127	
	Copy the backup DCT data file (*.mmdct) to the MAS.	125	
	Run MM_Setup from the desktop. The machine shuts down after the utility runs.	141	
	When the Modular Messaging Configuration Wizard launches, click **Next** on the Welcome screen. Select the backup DCT data file by selecting the file if it is displayed or by browsing to it.	119	
	Review the DCT data file and complete any empty fields. Save the file.	178	
	On the MAS Number screen, select the number of the MAS that you are recovering.	178	
	Complete the Windows Setup wizard and continue with the Modular Messaging Configuration Wizard. **Note:** The installation requests a restart after Net configuration and Windows does not auto logon. Instead, you are prompted with the Logon screen, where you need to press **Ctrl**+**Alt**+**Del** and click OK to continue with the logon and the installation.		
	Install the User Administration Extensions at this time onto the Messaging Application Server.	40	

Table 19: Avaya MAS restore procedure

✔	Procedure	Page	Comments
	For a system with an Exchange 2003 peer mail server, install Exchange System Management Tools.	46	
	For a system with an Exchange 2003 peer mail server, install Exchange Server 2003 SP2.	46	
	For a system with an Exchange 2007 peer mail server, install Exchange 2007 Management Tools and additional required software.	46	
	For a system with Exchange 2007, install Microsoft Exchange Server 2007 Service Pack 1	46	
	For a system with Exchange 2010 peer mail server, install MAPI Client, PowerShell 2.0 and additional required software.	52	
	Install antivirus software.	52	
	Complete the configuration wizard.		
	Administer antivirus software.	52	
	Install Modular Messaging software updates.	55	
	Update Microsoft Windows.	46	Follow site-specific procedures.
	Disable the private LAN.	55	
	Enter RAS IP address on the MAS	56	
	Install Modular Messaging Active Directory Exchange extensions on the MAS.	41	
	Configure port boards, if necessary.	309	Step is required only for port boards that do not use one of the automatic-configuration switch integrations. This is first step in port board configuration. Configuration is completed later in procedure.

Table 19: Avaya MAS restore procedure

✔	Procedure	Page	Comments
	Restore customer data including: • customized tone files • customized prompt files • caller applications • SIP certificate files • WSO system services data file • Audit database • Operation history and transaction databases	119	
	Specify the preferred language for the MAS.	81	For a non-English Windows operating system.
	Install and configure WebLM server	89	
	Obtain and apply PLDS license for this system	91,91	
	Configure MAS-specific parameters: • INADS alarming, if used • Port boards • Switch integration	99	
	Restart messaging service.	102	
	Verify call-handling capability.	104	
	Verify alarming setup.	104	
	Verify Tracing Service operation, if you installed Tracing Server software on this server.	105	
	Verify Audit Service	106	
	Run all acceptance tests that are relevant to the system.	112	
	Back up the MAS using the regular backup procedures for this site. Be sure to include the revised DCT data file in this backup.	119	
	Run the following tests: • Disk defragmenter system tool • chkdsk command	120	
	Complete steps necessary to turn the system over to the customer.	120	

Recovering from a catastrophic disk failure on a customer-provided MAS

Overview

There may be site-specific requirements and procedures for recovering from a catastrophic disk failure. Use the procedures appropriate to your site. The following is one procedure that can be used to recover the customer-provided MAS.

In summary, to restore a customer-provided MAS you will need to:

1. Replace the failed drive.
2. Configure a network card to support the corporate LAN connection
3. Manually join the Windows domain
4. Install and enable Windows services
5. Install and run the Modular Messaging Configuration Wizard
6. Administer antivirus software
7. Install Modular Messaging Active Directory Exchange extensions
8. Restore customer data
9. Configure the voice mail system
10. Configure services
11. Perform acceptance tests on the entire system.
12. Back up the restored system and hand it off to the customer.

Table 20: customer-provided MAS restore procedure on page 338 lists the steps necessary to restore a customer-provided MAS. It contains page references to detailed instructions for each step.

Requirements for restore of customer-provided MAS

To successfully restore a system to Modular Messaging Release 5.2, you need:

- A replacement hard disk drive.
- Release 5.2 of the Modular Messaging application software.
  - *Avaya Modular Messaging Messaging Application Server Software* media. You must use the most recent version of the DVD. It is labeled: "Build 9.2 (GA) + SP 8".

  - *Avaya Modular Messaging Documentation.*

- The following information and software from the Avaya Support Web site at http://www.avaya.com/support. For more information about how to access these items on the Web site, see Obtaining the DCT data file on page 3.
  - The most current copy of the configuration notes for this switch integration.
  - Avaya software updates that are required to bring the Avaya Modular Messaging software up to date after a restore. Download this software to a USB storage device. For more information about downloading the updates, see Appendix E: Updating Modular Messaging software on page 303.
  - The latest copy of the DCT executable file (**MMDCT.exe**). Download the file from the Avaya support Web site to a USB storage device.
- Customer-provided Microsoft Exchange System Management Tools. (Microsoft Exchange 2003 System Management Tools are highly recommended. The procedures in this chapter describe installation with the 2003 tools.) When installing a system with Exchange 2007 peer mail servers, you will require the 32-bit version of the Exchange 2007 Management Tools and additional software downloads. For more information, see Installing third-party software for Exchange 2010 on page 72 and Installing third-party software for Exchange 2007 on page 73.
- Microsoft Exchange 2003 Service Pack 2 for Exchange 2003 System Management Tools.
- Access to the most recent backup DCT data file as well as any backup files that will need to be restored to the system.

To restore an MAS configuration with this procedure after a catastrophic disk failure, you must have a previously saved and updated DCT data file. For information about maintaining a current DCT data file, see Using the DCT to collect information from an MAS on page 130 or see the DCT online help system or its printed version, *Avaya Modular Messaging Data Collection Tool Help*, for a complete description of the procedure to analyze a system with the DCT executable file.

CAUTION:

You cannot restore the MAS without a DCT data file that was created by analyzing the system.

Include the updated DCT data file in any regular, scheduled backups administered for this site so that the file is available if needed for a restore.

Restoring the customer-provided MAS

To restore the MAS, complete the tasks in the following checklist. As you complete a task, make a check mark in the " ✔ "column. For additional information or detailed procedures, see the referenced page number.

Table 20: customer-provided MAS restore procedure

✔	Procedure	Page	Comments
	Download required Avaya software updates, including the latest version of the planning forms and the DCT executable file (**MMDCT.exe**).	4	Web access required.
	Collect any software media that is needed, such as Microsoft Windows updates or antivirus software.	54	Leave customer media on-site.
	Obtain and review the configuration notes for any changes.	4	
	Copy the backup DCT data file (**.mmdct*) to a USB storage device with the latest DCT executable file (**MMDCT.exe**).		
	For a system with an Exchange 2003 peer mail server, obtain the Exchange System Management Tools and Exchange 2003 Service Pack 2 from the customer. For a system with an Exchange 2007 peer mail server, download Management Tools and additional required software including MAPI Client, Powershell 1.0, Exchange 2007 Service Pack 1, Microsoft Management Console 3.0, and .NET 2.0 as needed. For a system with and Exchange 2010 peer mail server, obtain MAPI Client, PowerShell 2.0 and additional required software.	73	
	Obtain virus-checking software for the MAS if required.	6	Customer obtains.
	Replace the hard drive.		For instructions, see the manufacturer instructions.
	Install the Windows Server 2003 operating system.		
	Update Microsoft Windows software	66	

Table 20: customer-provided MAS restore procedure

✔	Procedure	Page	Comments
	Adjust system values: • Event Viewer values • File and Printer Sharing properties • Windows Server 2003 operating system values	62	
	Add the Modular Messaging customer account and technical support account to the local administrators group.	68	
	Install Microsoft Windows SP2.	62	
	Verify that the USB storage device with the DCT data file and most recent DCT executable file is inserted in the USB port.	69	
	Copy the backup DCT data file (*.*mmdct*) to a directory on the MAS.	69	
	Verify that all additional backup files that must be restored are at a location accessible to the MAS. This includes: • customized tone files • customized prompt files • caller applications • Avaya license files. • SIP certificate files • WSO system services data file • Audit database • Operation history and transaction databases	119	
	Log on to the MAS using the Modular Messaging customer account.		
	When the Modular Messaging Configuration Wizard launches click **Next** on the Welcome screen. Select the backup DCT data file by selecting the file, if displayed, or by browsing to it.	69	
	Review the DCT data file and complete any empty fields. Save the file.	69	
	On the MAS Number screen, select the number of the MAS that you are recovering.	70	
	Install the User Administration Extensions at this time onto the Messaging Application Server.	40	

Table 20: customer-provided MAS restore procedure

✔	Procedure	Page	Comments
	For a system with an Exchange 2003 peer mail server, install Exchange System Management Tools.	73	
	For a system with an Exchange 2003 peer mail server, install Exchange Server 2003 SP2.	73	
	For a system with an Exchange 2007 peer mail server, install Exchange 2007 Management Tools and additional required software including MAPI Client, Powershell 1.0, Microsoft Management Console 3.0 and .NET 2.0 as needed.	73	
	For a system with Exchange 2007, install Microsoft Exchange Server 2007 Service Pack 1	73	
	For a system with Exchange 2010 peer mail server, install MAPI Client, PowerShell 2.0 and additional required software.	52	
	Administer antivirus software.	54	
	Change LAN name and power management settings	75	
	Enter RAS IP addresses for this MAS	76	
	Set the logging location if other than default.	77	
	Administer antivirus software.	54	
	Install Modular Messaging Active Directory Exchange extensions on the MAS.	37	
	Configure port boards, if necessary.	309	Step is required only for port boards that do not use one of the automatic-configuration switch integrations. This is first step in port board configuration. Configuration is completed later in procedure.

Table 20: customer-provided MAS restore procedure

✔	Procedure	Page	Comments
	Restore customer data including: • customized tone files • customized prompt files • caller applications • SIP certificate files • WSO system services data file • Audit database • Operation history and transaction databases	119	
	Specify the preferred language for the MAS.	81	For a non-English Windows operating system.
	Install and configure WebLM server	89	
	Obtain and apply PLDS license for this system	91,91	
	Configure MAS-specific parameters: • INADS alarming, if used • Port boards • Switch integration	99	
	Restart MM Messaging Application Server service.	102	
	Verify call-handling capability.	104	
	Verify alarming setup.	104	
	Verify Tracing Service operation, if you installed Tracing Server software on this server.	105	
	Verify Audit Service	106	
	Run all acceptance tests that are relevant to the system.	112	
	Back up the MAS using the regular backup procedures for this site. Be sure to include the revised DCT data file in this backup.	119	
	Run the following tests: • Disk defragmenter system tool • chkdsk command	120	
	Complete steps necessary to turn the system over to the customer.	120	

Appendix J: Installing and configuring the AudioCodes gateway

This appendix describes how to install and configure the AudioCodes gateway.

The procedure has two parts:

Field Configuration: This procedure must be performed by a technician on the site where the PBX switch and the AudioCodes gateway are physically located. This procedure must be completed before you attempt to configure the AudioCodes gateway remotely.

Remote Configuration: This procedure can either be performed by a technician at a remote site using remote access tools or by the technician on the site where PBX and AudioCodes gateway are located.

Topics in this appendix include:

- Installation prerequisites on page 344
- Installing and configuring the AudioCodes gateway at switch location on page 345
- Continue configuring the AudioCodes gateway on page 348

Installation prerequisites

Ensure that you have the following before you start the AudioCodes gateway installation:

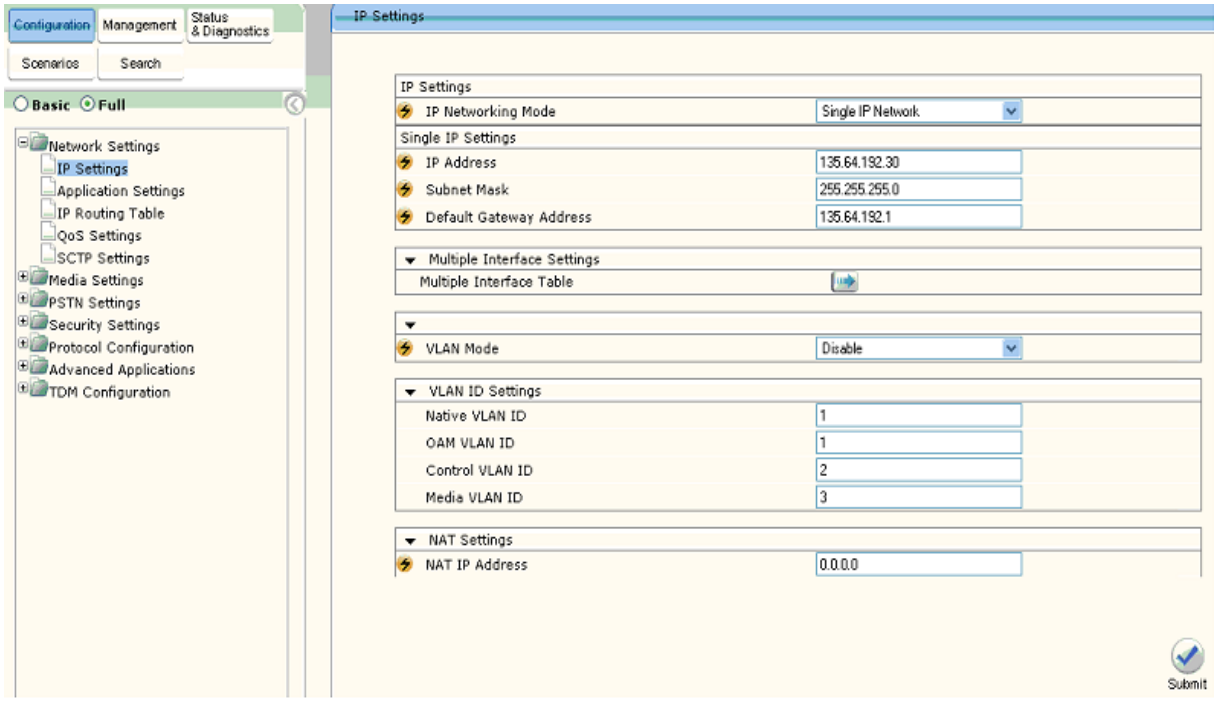
- DCT file and MM DCT tool (MMDCT.exe)
- AudioCodes gateway with interface modules required for this installation.
- Configuration notes for AudioCodes gateway downloaded from the AudioCodes Web site at http://www.audiocodes.com/avaya.
- Avaya PBX configuration note where required.
- Download AudioCodes firmware and details of the firmware version required for this installation from the AudioCodes Web site at http://www.audiocodes.com/avaya.
- The following information from the AudioCodes gateway configuration notes:
  - Cabling requirements
  - PBX configuration requirements. See section 3.0 of configuration notes for AudioCodes gateway.
- X-Over cable
- A laptop
- Machine on customer's corporate LAN with access to Internet Explorer used to configure the AudioCodes gateway.

Installing and configuring the AudioCodes gateway at switch location

Perform the following steps locally.

1. Configure the PBX. Use the configuration notes downloaded from the AudioCodes Web site.
2. Complete the PBX connection patching.
3. Complete ethernet connection patching.
4. Complete the following steps to physically install the gateway:
   a. Unpack the AudioCodes gateway.
   b. Mount the AudioCodes gateway in the rack.
   c. Connect the PBX to the AudioCodes gateway.
   d. Connect one end of the X-Over cable to the left Ethernet port on the AudioCodes gateway.
5. Prepare the computer for initial AudioCodes gateway configuration:
   a. Connect the other end of X-Over cable to the NIC on the laptop.
   b. Change the IP Address of the computer using the following steps:
      1. Open Control and double-click Network Connections. The system opens the **Network Connections** window.
      2. Select the LAN connection, right-click and select **Properties**.
      3. In the **General** tab, click **Internet Protocol (TCP/IP)**.
      4. Click **Use the following IP address** and change the IP address to 10.1.10.11.
      5. Click **OK**.
      6. Close all open Windows.
   c. Launch the Internet Explorer (IE) and complete the following to clear the proxy server settings.
      1. Click **Tools > Internet Options**.
      2. In the **Internet Options** dialog box, click **Connections** tab.
      3. Click LAN Settings. The system opens Local Area Networks (LAN) Setting dialog box.
      4. Clear the **Use a proxy server for your LAN** check box.
      5. Click **OK** to close IE and for the changes to take effect.

Figure 10: Configuring AudioCodes gateway



6. Complete the initial IP configuration of the AudioCodes gateway:
   a. Launch Internet Explorer.
   b. Enter 10.1.10.10 in the IE address bar. This is the factory default IP address for the Audiocodes gateway.
   c. When prompted, enter ***Admin as*** the account name and the password. Note that the account name and password are case-sensitive.

      The system opens the AudioCodes Gateway WebAdmin Home Page.
   d. Click the **Configuration** tab on the left pane.
   e. Click **Full**.
   f. Expand **Network Settings** by selecting the **+** symbol.
   g. Click **IP Settings**.

      The system displays **IP Settings** page.
   h. In the **IP Networking Mode** field, click **Single IP Network**
   i. Change the **IP Address** to the value assigned to the gateway for your network.
   j. Change the **Subnet Mask** to match the subnet mask for your network.
   k. Change the **Default Gateway Address** to match the default gateway for your network.
   l. Click **Submit** to save the changes.

WARNING:

Ensure that you *do not* disconnect the power to the AudioCodes gateway at this stage. If you disconnect the power, you loose the changes made to IP Address, until you save the settings in step 4d described in Continue configuring the AudioCodes gateway on page 348.

If the power to the device is disconnected then the IP Address changes will be lost until we reach step x, the step where the burn occurs

Note:

When you submit the changes, the connection between the AudioCodes gateway and the computer is lost. Therefore, you must complete step 7 before you continue. You can now set the computer back to its original network configuration.

7. Connect the AudioCodes gateway to the network.
   a. Remove X-Over cable from the Ethernet port on the AudioCodes gateway.
   b. Connect the network cable for the customers corporate LAN to the first Ethernet port on the AudioCodes gateway.
8. Connect to the AudioCodes Gateway WebAdmin from the machine which is connected to the customer's corporate LAN.
   a. On the machine connected to the customer's corporate LAN, launch IE.
   b. In the IE Address bar, enter the IP Address for the AudioCodes gateway.

      The IP Address you enter is the one you configured in step 6i.
   c. When prompted, enter ***Admin*** *as* the account name and the password.

      The system opens the AudioCodes Gateway WebAdmin Home Page.
9. Update Administrative password for the gateway:
   a. In the left pane, expand **Security Settings.**
   b. Click **WEB User Accounts**.
   c. Click **Change Password**.
   d. Set the gateway Admin account name if required.
   e. Set the Admin password to the value that is provided in the DCT data file.
   f. Click **Submit.**

Continue configuring the AudioCodes gateway

Complete the following steps to configure the AudioCodes gateway locally or from a location remote to the Audiocodes gateway:

Note:

Ensure that you have the required AudioCodes gateway, Avaya Modular Messaging and PBX configuration notes available.

1. Connect to the customer site using the standard remote access method, if required.
2. Complete the following steps from the machine referred in Installation prerequisites on page 344, to connect to the AudioCodes gateway:
   a. Launch Internet Explorer (IE).
   b. In the IE Address bar, enter the IP address for the AudioCodes gateway
   c. When prompted, enter the account name and the password set by the field technician as outlined in Installing and configuring the AudioCodes gateway at switch location on page 345.

   The system opens the AudioCodes Web Admin Home Page.
3. On the AudioCodes Gateway Home page, confirm that the gateway firmware version matches with that provided in section 1.2 of the AudioCodes gateway configuration notes.
4. If the Firmware loaded on the gateway does not match the required version, then complete the following steps:
   a. Click **Device Actions > Software Upgrade Wizard**.
   b. Click **Browse** and locate the Firmware ***.CMP*** file.
   c. Click **Next**.
   d. Click **Burn** to save the changes to flash memory**.**
   e. Click **Device Actions > Reset**.
5. Make the required changes in the ***template.INI*** file using the steps described in AudioCodes configuration notes.
6. Upload the ***template.INI*** file to the gateway:
   a. Click **Device Actions > Load INI file.**
   b. Click **Browse** and locate the ***template.INI*** file.
   c. Click **Load INI file.** The system displays a warning message, when the system prompts you, click **OK**.
7. If the customer is non-US and switch integration type is *Analog*, you may upload the ***.CPT*** file that is specific to a region to the gateway:
   a. On the left pane, click the **Management** tab.

b. Expand **Software Update.**

c. Click **Load Auxiliary Files**. The system opens **Load Auxiliary Files** page.

d. In the **Call Progress Tones files** field, click **Browse** and select the appropriate ***.CPT*** file.

e. Click **Load File**.

f. Click **OK**.

Call Progress Tones (CPT) file is a region-specific and telephone exchange-dependent file. The file contains the call progress tone (CPT) levels and frequencies that the device uses. The default CPT file is **U.S.A**.

8. In the AudioCodes Web Admin Home Page, verify that the AudioCodes gateway configuration matches with the details provided in section 4 of AudioCodes gateway configuration notes.
9. Configure the Avaya MASs in Modular Messaging system.

   Use section 5 in AudioCodes gateway configuration notes as a guide to configure MASs. If you add a new MAS to your VMD, then you may need to update the Audiocodes gateway configuration for the added MAS.
10. Perform the acceptance tests on MASs using the AudioCodes gateway you have just configured as described in Performing acceptance tests on page 112.

Appendix K: Administrator reference

This appendix details the permissions and data schema modifications that are required to support Modular Messaging software in a Microsoft Exchange environment.

Exchange 2003, 2007, and 2010 group permissions

Avaya Modular Messaging customer account permissions are covered in Assigning permissions to the Modular Messaging service permissions group on page 17. This section details why the Modular Messaging customer account must be added to the following groups:

- The BuiltIn/Account Operators group in each domain that contains accounts that will be enabled for Avaya Modular Messaging. This ensures that the Modular Messaging software has rights to perform the following operations:
  - Provide full access to the ms-Exch-Extension-Data attribute for user objects that are to be enabled for Modular Messaging. This access right is required to enable Modular Messaging subscriber accounts.
  - Create container objects. Avaya Modular Messaging creates a voice mail domain container. By default, the voice mail domain container is located at the root of the domain for which the Modular Messaging customer account is a member. This container stores the directory objects required for the Messaging Application Server and Mailbox Monitor Server software components.

    If the Modular Messaging customer account does not have sufficient privileges to create container objects at the base location of the domain that contains the customer account, a voice mail domain container must be created manually.
  - Create User objects, and mailbox-enable User objects, in the voice mail domain container. This right is required for the operation of the Messaging Application Server and Mailbox Monitor Server software.
- The BuiltIn/Administrators group in the domain that contains the Global Catalog servers, that will be used as peer-directory servers for Avaya Modular Messaging servers. This can be the domain that contains the customer account, or any sub-domain that contains the customer account. The right enables the Modular Messaging software to obtain search results from the peer-directory server, including recently deleted objects. This allows Avaya Modular Messaging to maintain consistency in its Front End Database (FEDB).
- The BuiltIn/Exchange Recipient Administrators group gives Modular Messaging full control of Exchange properties on Active Directory user objects and is required to manage mailbox settings for Modular Messaging. Modular Messaging requires membership in this group only in an environment with an Exchange 2007 peer mail server.

- The Recipient Management and Public Folder Management groups give Modular Messaging full control of Exchange properties on Active Directory user objects. Both groups are required to manage mailbox settings for Modular Messaging. Modular Messaging requires membership in this group only in an environment with an Exchange 2010 peer mail server.

The following table details the property permissions required to support Modular Messaging and their purpose. It also indicates the lowest level in the Exchange Service property tree that this permission should be applied. Parentheses indicate permission names with an Exchange 2007 and Exchange 2010 system.

Table 21: Required switch and messaging information

Permission	Description	Applies to this object and subcontainers	Modular Messaging requirement
Read	Read permission for items in container	Mailbox Store	Core requirement
Execute	Execute permission for items in container	Mailbox Store	Automatic with “Read”
Read Permissions	Ability to read the permissions for an object	Mailbox Store	Automatic with “Read”
Create Children (Create all child objects)	Ability to create an object below the current object	Connectors	Octel Analog Networking
List Contents	Displays the contents and children of an object	Exchange Organization	Exchange System Manager
Read Properties (Read all properties)	Allows for Properties to be read from the class object	Administrative Group	Core requirement
Write Properties (Write all properties)	Allows for existing class object Properties to be written to	Connectors	Octel Analog Networking
Administer Information Store	Allows creation of objects at root of folder	Mailbox Store	Voicemail Domain Mailbox
Create Named Properties in the Information Store	Allows new properties to be added to the class object	Mailbox Store	User Admin
View Information Store Status	Required for MAPI Logon	Mailbox Store	External Caller Mailbox

Table 21: Required switch and messaging information

Permission	Description	Applies to this object and subcontainers	Modular Messaging requirement
Receive As	Receive on behalf of privilege	Mailbox Store	Core requirement
Send As	Send on behalf of privilege	Mailbox Store	Core requirement

Send As permission

You must assign *Send As* permission to the Modular Messaging service permissions group to allow Modular Messaging to deliver call answer messages to Modular Messaging enabled mailboxes. For procedures for assigning *Send As* permission see Assigning Send As permission on page 17.

Previously *Send As* permission was included when *Full Mailbox Access* was granted to a user. However, in current and future fixes and releases of Exchange 2003, 2007, and 2010 *Send As* permission must be added separately to the Modular Messaging service permissions group. If it is not, any Exchange server with the most recent Microsoft patches applied will not be able to deliver call answer messages to Modular Messaging enabled mailboxes. Messages in the Spool folder cannot be delivered and will be continually retried. Additionally, users that log into the TUI will not be able to send messages to other users and will receive a *Message Cancelled* statement from the system.

Send As permission is added at the Root of the Forest to allow it to populate to every object in the Forest. However distribution is dependent on restrictions within the Forest. By default inheritance throughout the Forest is enabled for basic users. However, if inheritance has been disabled anywhere in the Forest, a user object will not receive *Send As* permission. In this case, inheritance must be enabled or *Send As* permission must be applied to that specific user.

Additionally, the accounts and groups listed below are protected by a background process that periodically checks and applies a security descriptor based on the AdminSDHolder object. This process removes Send As permission from these groups and members and reverts back to permissions configured for the AdminSDHolder object. Therefore the Send As permission must be added to the AdminSDHolder object using the Dsacls.exe utility if an account belonging to any of the protected groups is Modular Messaging enabled. For details on this procedure, see Assigning Send As permission on page 17.

Protected Groups and users:

- Administrators
- Account Operators
- Server Operators
- Print Operators
- Backup Operators
- Domain Admins
- Schema Admins
- Enterprise Admins
- Cert Publishers
- Administrator account
- Krbtgt account

Active Directory schema updates

Avaya Modular Messaging software requires the following changes to be made to the schema in an Exchange environment before any other Modular Messaging server components are installed, you must:

- Enable replication of the ms-Exch-Extension-Data attribute in the Global Catalog.
- Increase the maximum amount of data that can be stored in the ms-Exch-Extension-Data attribute to 64KB. This increased storage is used for G7.11 audio encoding format, which is typically used only on systems that support Teletypewriter (TTY).
- Add classes and attributes for Octel Analog Networking (if applicable).

The Modular Messaging software stores information about subscriber configurations in the ms-Exch-Extension-Data attribute. So that Modular Messaging MASs can obtain this information, this attribute must be replicated in the Global Catalog, a central repository for information about objects in the Windows 2000 or 2003 forest. When the replication is enabled, the system instructs the Global Catalog servers to include the ms-Exch-Extension-Data attribute in the list of objects replicated in the Windows 2000 or 2003 forest.

Replication of the ms-Exch-Extension-Data in the Global Catalog is also necessary for the correct operation of the Modular Messaging Client software (formerly called the Subscriber Options package). This is because the MAPI address book provider for Active Directory uses the Global Catalog as its data source. Replication is required for MAPI to support access to client applications, such as the MM Client software, through the PR_EMS_AB_EXTENSION_DATA property.

When the Modular Messaging Subscriber Administration extensions software component is installed, the software makes the following changes:

- Adds a Modular Messaging property page for each user in Active Directory Users and Computers. More specifically, the guide “A6688A44-CEDE-456E-AE57-3567D9909AE7” is added to the multi-valued attribute adminPropertyPages on the user-Display object, which has the dn: CN=user-Display,CN=409, CN=DisplaySpecifiers,CN=Configuration,DC=mycorp,DC=com.
- Copies files for the software components required to display the Modular Messaging property page to the Program Files\Avaya Modular Messaging directory.

Appendix L: Migrating Modular Messaging to Exchange 2007

This appendix describes how to install Modular Messaging in a network with Exchange 2007 mail servers or a combination of Exchange 2003 and 2007 mail servers. Select the procedure that describes your environment:

- Installing Modular Messaging with Exchange 2007 on page 358

  Provides instructions for installing a new Modular Messaging system in a network that contains either only Exchange 2007 mail servers, or a combination or Exchange 2003 and 2007 mail servers.

- Installing Modular Messaging with a separate Exchange 2007 VMD on page 360

  Provides instructions for installing a new Voice Mail Domain (VMD) in an existing Modular Messaging system where the new VMD will use an Exchange 2007 server as the peer mail server.

- Migrating Modular Messaging to Exchange 2007 on page 363

  Provides instructions for migrating an existing Modular Messaging system from Exchange 2003 mail servers to use Exchange 2007 servers as the peer mail servers. In most cases it is the eventual goal to remove the Exchange 2003 servers.

Installing Modular Messaging with Exchange 2007

Use the instructions in this section to install a new Modular Messaging system in a corporate infrastructure with Exchange 2007 mail servers or a combination of Exchange 2003 and 2007 mail servers.

Installation requirements

The installation requires the following:

- All Exchange servers must be functioning correctly
- You must have the following software available during the installation:
  - Microsoft Exchange Server MAPI Client
  - Microsoft Exchange 2007 Management Tools, 32-bit version
  - Microsoft Exchange Server 2007 Service Pack 1
  - During the installation you may be required to install additional components on your system if they have not been previously installed. These include Powershell 1.0, Microsoft Management Console 3.0, and .NET 2.0
  - Modular Messaging Release 5.2 Service Packs and patches

  For additional information about downloading Modular Messaging Service Packs and patches, see Appendix E: Updating Modular Messaging software on page 303.
- These instructions assume that the peer mail server is running Exchange 2007, and that Modular Messaging has never been installed in the Exchange organization.

What's new with Exchange 2007

During the installation follow all the procedures in the chapters of this book that describe how to install, configure and test a Modular Messaging system including those in Chapter 4: Configuring an Avaya MAS on page 45 or Chapter 5: Configuring a customer-provided MAS on page 59. However, note the following procedures that have changed when installing Modular Messaging with an Exchange 2007 peer mail server:

- The customer account group must be a member of the *Administrators, Account Operators,* and *Exchange Recipient Administrator* groups. Also, the permissions assigned to the customer account group differ with Exchange 2007. Follow the procedures in Chapter 2: Preparing to install Modular Messaging software on page 9 to set up the Modular Messaging accounts and assign permissions.

- Microsoft provides a PowerShell command that you can use to automate many of the steps needed to create and assign permissions to the customer account group. For more information, see Using Power Shell to create a Modular Messaging service permissions group on page 16.
- Exchange 2007 does not support Octel Analog Networking (OAN). Follow the procedures in Updating the Active Directory on page 35. Do not select the check box to enable Octel Analog Networking.
- The NNTP and SMTP services are not required for Exchange 2007 Management Tools. See Installing and enabling Microsoft Windows services on page 64.
- When installing third-party software, you must install the 32-bit version of Exchange 2007 Management Tools and additional software and Microsoft Exchange Server 2007 Service Pack 1. For more information, see Installing third-party software on page 181.
- An MAS that is configured to communicate with an Exchange 2007 peer mail server also can be used to monitor Exchange 2003 non-peer mail servers. To do this you must create a monitor mailbox for each Exchange 2003 non-peer mail server you want to monitor. For more information, see Creating the non-peer Exchange 2003 monitor mailbox on page 369.
- When installing Avaya software updates, be sure to include the most recent Modular Messaging Release 5.2 service packs and patches.

Installing Modular Messaging with a separate Exchange 2007 VMD

Use the instructions in this section to install a new Modular Messaging system into a new Voice Mail Domain (VMD) that will be hosted on Exchange 2007 where there is already an existing VMD hosted on Exchange 2003 in the same Exchange organization.

Installation requirements

The installation requires the following:

- All Exchange servers must be functioning correctly
- Microsoft Exchange transport between Exchange 2003 servers and Exchange 2007 servers must be functioning correctly
- Modular Messaging Release 3.0, 3.1, or 4.0 is running on all MASs and supplementary servers in the existing VMD and is functioning correctly
- You must have assigned *send as* permission to the customer account group for the existing VMD. For instructions, see Assigning Send As permission on page 17.
- You must have the following software available during the installation:
  - Microsoft Exchange Server MAPI Client
  - Microsoft Exchange 2007 Management Tools, 32-bit version
  - Microsoft Exchange Server 2007 Service Pack 1
  - During the installation you may be required to install additional components on your system if they have not been previously installed. These include Powershell 1.0, Microsoft Management Console 3.0, and .NET 2.0
  - Modular Messaging Release 5.2 Service Packs and patches

  For additional information about downloading required Microsoft software, see Installing third-party software on page 181. For additional information about downloading Modular Messaging Service Packs and patches, see Appendix E: Updating Modular Messaging software on page 303.
- These instructions assume that when you begin the installation:
  - Modular Messaging MASs in the existing VMD are using Exchange 2003 servers as peer mail servers
  - All Modular Messaging user Exchange mailboxes in the existing VMD are located on Exchange 2003 servers

Note:

Subscribers in the existing Modular Messaging 3.0 VMD hosted by 2003 mail servers cannot be assigned mailboxes in the new VMD hosted on Exchange 2007 until all MASs in the existing VMD are upgraded to Modular Messaging Release 5.2.

What's new with Exchange 2007

During the installation follow the procedures in Chapter 4: Configuring an Avaya MAS on page 45 or Chapter 5: Configuring a customer-provided MAS on page 59 as well as procedures to configure and test the Modular Messaging system. However, note the following procedures that have changed when installing Modular Messaging with an Exchange 2007 peer mail server:

- You must add the customer account group to the *Exchange Recipient Administrator* group. See Creating the Modular Messaging customer account on page 11 for instructions for adding the customer account group to the *Exchange Recipient Administrator* group.
- The NNTP and SMTP services are not required for Exchange 2007 Management Tools. See Installing and enabling Microsoft Windows services on page 64.
- When installing third-party software, you must install the 32-bit version of Exchange 2007 Management Tools, Microsoft Exchange Server 2007 Service Pack 1, and additional software. For more information, see Installing third-party software on page 181.
- If you will be using an MAS with an Exchange 2007 peer mail server to monitor an Exchange 2003 non-peer mail server, you must create a non-peer mail server monitor mailbox. For more information, see Creating the non-peer Exchange 2003 monitor mailbox on page 369.
- When installing Avaya software updates, be sure to include the most recent Modular Messaging Release 5.2 service packs and patches.

Continuing the installation

After the new Modular Messaging VMD has been installed and tested, complete the following optional procedures. These procedures are not required as part of the installation procedure. They can be completed now or over time in the future.

1. Move Modular Messaging enabled mailboxes to the Exchange 2007 mail server. For more information, see Moving mailboxes to the Exchange 2007 server on page 365.
2. Move Modular Messaging enabled mailboxes to the Exchange 2007 VMD. For more information, see Moving mailboxes to a new Exchange 2007 VMD on page 362.

Moving mailboxes to a new Exchange 2007 VMD

To move Modular Messaging enabled Exchange mailboxes to the new Exchange 2007 VMD:

1. Click **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** window, expand the directory for the Modular Messaging Windows domain and select the VMD that contains the mailboxes that you want to move.
3. In the right pane, double-click the mailbox you want to move to the new VMD.
4. In the **Properties** window, click the **Modular Messaging** tab.
5. In the **Voice mail domain** field, select the new VMD from the drop-down list.
6. Click **OK** to save changes and close the **Properties** window. Close the **Active Directory Users and Computers** window.
7. Right-click **My Computer** and select **Manage**.
8. In the **Computer Management** window, in the left pane, expand **Event Viewer**.
9. Refresh the window display periodically until you see a **1027** event (gv_vserver) reporting that the FEDB update has occurred.
10. Test the functionality of the moved mailbox using the telephone user interface (TUI) and client software.
11. Repeat this procedure for each mailbox you are moving to the new VMD.

    Note:

    You can also use the VMEnable tool to bulk move Modular Messaging mailboxes to the new VMD.

Migrating Modular Messaging to Exchange 2007

Use the instructions in this section to migrate an existing Modular Messaging system from Exchange 2003 peer mail servers to use Exchange 2007 peer mail servers. In most cases it is the eventual goal to remove the Exchange 2003 servers.

Installation requirements

The installation requires the following:

- All Exchange servers must be functioning correctly. Exchange 2007 servers are installed and fully tested.
- Modular Messaging Release 5.2 is running on all MASs and supplementary servers and is functioning correctly
- You must have the following software available during the installation:
  - Microsoft Exchange Server MAPI Client
  - Microsoft Exchange 2007 Management Tools, 32-bit version
  - Microsoft Exchange Server 2007 Service Pack 1
  - During the installation you may be required to install additional components on your system if they have not been previously installed. These include Powershell 1.0, Microsoft Management Console 3.0, and .NET 2.0
  - Modular Messaging Release 5.2 Service Packs and patches

  For additional information about downloading Modular Messaging Service Packs and patches, see Appendix E: Updating Modular Messaging software on page 303.
- These instructions assume that when you begin the migration:
  - Modular Messaging MASs are using Exchange 2003 servers as peer mail servers
  - All Modular Messaging user Exchange mailboxes in the existing VMD are located on Exchange 2003 servers
  - There are no Exchange 5.5 servers in the environment

What's new with Exchange 2007

Complete the following procedures when migrating Modular Messaging to the Exchange 2007 mail server:

- You must add the customer account group to the *Exchange Recipient Administrator* group. See Creating the Modular Messaging customer account on page 11 for instructions for adding the customer account group to the *Exchange Recipient Administrator* group.
- If you have not previously assigned *send as* permissions to the customer account group, do so now. For instructions, see Assigning Send As permission on page 17.
- After adding the new group and assigned *send as* permissions, restart all MASs and supplementary servers to populate permission changes to all MASs.
- If you will be using an MAS with an Exchange 2007 peer mail server to monitor an Exchange 2003 non-peer mail server, you must create a non-peer mail server monitor mailbox. For more information, see Creating the non-peer Exchange 2003 monitor mailbox on page 369.

Continuing the installation

Migrate the Modular Messaging system to the Exchange 2007 mail servers by completing the following procedures:

1. Optionally move Modular Messaging enabled mailboxes to the Exchange 2007 mail server. This step is not required as part of the installation procedure. It can be completed now or over time in the future. For more information, see Moving mailboxes to the Exchange 2007 server on page 365.
2. Assign the MASs to the Exchange 2007 peer mail servers. For more information, see Assigning MASs to Exchange 2007 peer mail server on page 366.
3. When you are ready to remove the Exchange 2003 servers from the Exchange organization, verify that there are no Modular Messaging MASs that are using them as their peer mail server. For additional information, see the *Servers Tab* section of the *Modular Messaging online help*. Also remove non-peer monitor mailboxes. Follow the Microsoft recommended procedures to remove the Exchange 2003 servers from the Exchange organization. The Exchange 2003 servers do not need to be removed as part of the installation procedure. They can be removed at any time in the future.

Moving mailboxes to the Exchange 2007 server

To move Modular Messaging enabled Exchange mailboxes to the Exchange 2007 server:

1. Click **Start** > **All Programs**> **Microsoft Exchange Server 2007**> **Exchange Management Console**.
2. In the left panel, select **Recipient Configuration**.
3. In the center panel, select the mailboxes that you want to move.
4. In the right panel, click **Move Mailbox**.
5. In the **Move Mailbox** window, in the **Server** field, select the name of the Exchange 2007 server you want to host the mailbox.
6. Click **Next** and follow the prompts to complete the Move Mailbox wizard.
7. Test the functionality of the moved mailbox using the telephone user interface (TUI) and client software.
8. Repeat this procedure as needed to move mailboxes to the Exchange 2007 mail server. It is not necessary to move all mailboxes immediately. Migration to the server can be phased.

   Note:

   You can also use the Exchange Shell move_mailbox command to move mailboxes, or the Exchange Shell script move_mailbox command to bulk move mailboxes. For additional information, see your Microsoft Exchange documentation.

Assigning MASs to Exchange 2007 peer mail server

Complete the procedures in this section only when you are ready to remove your Exchange 2003 peer mail servers and replace them with Exchange 2007 peer mail servers. To move the MASs to the Exchange 2007 peer mail server, you must:

- Install Exchange 2007 Management Tools on the MAS. See Installing Exchange 2007 Management Tools on page 366.
- Change the MAS to access the Exchange 2007 peer mail server. See Changing to the Exchange 2007 peer mail server on page 368.

Move and test each MAS separately. It is not necessary to move all MASs to the Exchange 2007 peer mail servers at the same time.

Required software

The following software downloads are required:

- Microsoft Exchange Server MAPI Client. The MAPI Client can be downloaded from the following site:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=e17e7f31-079a-43a9-bff2-0a110307611e&DisplayLang=en

- Microsoft Exchange 2007 Management Tools, 32-bit version. Downloaded the file from:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=444C259E-605F-4A82-96D5-A2F448C9D4FF&displaylang=en

- Microsoft Exchange Server 2007 Service Pack 1
- During the installation you will be required to install additional components on your system if they have not been previously installed. These include Powershell 1.0, Microsoft Management Console 3.0, and .NET 2.0. The installation of the Management Tools will guide you through the installation of the required components and patches.

Installing Exchange 2007 Management Tools

Modular Messaging requires the 32-bit version of the Exchange 2007 Management Tools. To upgrade your MASs to the new management tools, complete the following steps:

1. Record which Modular Messaging services are running on the MAS.
2. Navigate to the **C:\Avaya_Support\tools\servicecontrol** directory.
3. Double-click the **StopMMServices.exe** file to stop all services on the MAS.

4. Uninstall the Exchange 2003 System Management Tools:
   a. Click **Start** > **Control Panel** > **Add or Remove Programs**.
   b. In the **Add or Remove Programs** window, select **Microsoft Exchange** and click **Change/Remove**.
   c. Complete the Microsoft Exchange Installation Wizard to remove the Exchange 2003 Management Tools.
5. Install Microsoft Exchange 2007 Management Tools:
   a. Double-click the tools executable file.
   b. Double-click the extracted Microsoft Exchange Installation wizard.
   c. Complete the Microsoft Exchange Installation Wizard selecting **Custom Exchange Server Installation**. Elect to install the **Management Tools**. For details about this procedure, see the Microsoft Exchange documentation.

   You may be prompted to download and install additional components and hotfixes. Follow the installation prompts. Be sure to download the Windows 2003 32-bit version of each component.
6. If prompted, restart the system.
7. Install the MAPI Client by double-clicking the MAPI executable file.
8. Verify that the Exchange 2007 Management Tools are working by completing the following procedure:
   a. Click **Start** > **All Programs**> **Microsoft Exchange Server 2007**> **Exchange Management Console**.
   b. Expand **Recipient Configuration** > **Mailboxes**.
   c. Verify that all Exchange mailboxes are listed.
9. Install Microsoft Exchange Server 2007 Service Pack 1.
10. Restart services by completing the following steps:
    a. Click **Start** > **Run** to open the **Run** window.
    b. In the **Open** field, type the following and press **Enter**:

       C:\Avaya_Support\Scripts\serverrecovery.vbs

Changing to the Exchange 2007 peer mail server

Use the Voice Mail System Configuration program to change the peer mail server for the MAS to the Exchange 2007 mail server:

1. On the MAS, launch the **Voice Mail System Configuration** program.
2. Expand **Message Application Servers** and the name of the MAS you are moving.
3. Under the MAS name, double-click **Messaging**.
4. On the **Messaging** window **General** tab in the **Mail Server Name** field, enter the name of the Exchange 2007 peer mail server.
5. Click **OK** to save the change and close the **Messaging** window. Close the VMSC window.
6. Navigate to the **C:\Avaya_Support\Tools\ServiceControl** directory.
7. Double-click the **StopMMServices.exe** file to stop all services on the MAS.
8. Using the Move Mailbox wizard on the Exchange Management Console, move the VMD mailbox from the old Exchange 2003 server to the new Exchange 2007 peer mail server. Complete this step only once for the Voice Mail Domain (VMD). For more information about moving mailboxes, see Moving mailboxes to the Exchange 2007 server on page 365.
9. Using the Move Mailbox wizard on the Exchange Management Console, move the External Caller mailbox from the old Exchange 2003 server to the new Exchange 2007 peer mail server. For more information about moving mailboxes, see Moving mailboxes to the Exchange 2007 server on page 365.
10. Restart all services by running the **serverrecovery.vbs** script. (If you have installed the patch, it will automatically restart services.)
11. Verify that the correct services are running on the MAS.
12. Repeat the steps in Installing Exchange 2007 Management Tools on page 366 and Changing to the Exchange 2007 peer mail server on page 368 for each MAS you are moving to the Exchange 2007 peer mail server. It is not necessary to move all the MASs at the same time.
13. After moving all required MASs to the Exchange 2007 peer mail server, perform a complete DCT analysis of the supplementary server and all MASs. All MASs, the supplementary server if one is present, and the Exchange message store must be running. For more information, see:
    - Using the DCT to collect information from an MAS on page 130 for an Avaya MAS
    - Using the DCT to collect information from an MAS on page 152 for a customer-provided MAS

Creating the non-peer Exchange 2003 monitor mailbox

If you will be using an MAS with an Exchange 2007 peer mail server to monitor a new Exchange 2003 non-peer server, complete the following steps to create the non-peer Exchange monitor mailbox:

1. Copy the file **C:\Avaya_Support\Exchange2007Migration\Add-Monitor-Mbx.exe** from the MAS to a machine that is running the Exchange 2003 System Management Tools.

   Note:

   This can be an Exchange 2003 server running the Exchange 2003 System Management Tools, or a machine with the Exchange 2003 System Management Tools that is used to administer the Exchange servers.

2. Click **Start > Run**, enter **cmd** and click **OK**.
3. In the command window, enter the following:

   Add-Monitor-Mbx *<Exchange server>* *<peer directory server>* *<Octel container>*

   where:

   <Exchange server> is the name of the non-peer Exchange 2003 server you want to monitor.

   <peer directory server> is the peer directory server used by the MASs

   <Octel container> is an optional entry that is not required if you are using the default Octel container location. Enter the location of the Octel container if you are not using the default location. For example: **cn=octel,cn=avaya,DC=ncis,DC=local**

   The non-peer Exchange server monitor mailbox is created. MASs will start monitoring the non-peer Exchange server when mailboxes located on the server are Modular Messaging enabled.

Appendix M: Migrating Modular Messaging to Exchange 2010

This appendix covers two topics: migrating a Modular Messaging system to Exchange 2010 and moving the mailboxes of existing subscribers to Exchange 2010.

To migrate the Modular Messaging system from server running Exchange 2007 or Exchange 2003 to a server running Exchange 2010, you need to perform three main tasks:

- Change the Peer Exchange Servers to Exchange 2010
- Move the VMD mailbox to Exchange 2010
- Move the Fax mailbox to Exchange 2010

You can migrate the existing subscriber mailboxes to Exchange 2010 servers without moving the VMD mailbox. This allows for flexibility in the migration strategy. You do not need to move all subscribers at the same time. You can move them in a phased manner.

To move the mailboxes, perform the procedure Moving Subscriber Mailboxes to Exchange 2010 on page 384.

But before starting, read the Installation prerequisites on page 372 and complete the steps listed in Preparing Exchange 2010 on page 374 before starting.

Migrating Modular Messaging to Exchange 2010

Use the instructions in this section to migrate an existing Modular Messaging system from Exchange 2003 mail servers to use Exchange 2010 servers, or from 2007 mail servers to use Exchange 2010 servers as the peer mail servers.

Installation prerequisites

Before you begin with any process the following must be true:

- All Exchange servers are functioning correctly.
- Exchange Server 2010 Service Pack 1 or later is installed and fully tested.
- Modular Messaging Release 5.2 is running on all MASs and supplementary servers and functioning correctly.
- Modular Messaging Release 5.2 Service Pack 6 or later is installed on each MAS and supplementary server. For the detailed steps for installing the update, see the Release Notes.
- PowerShell 2.0 is installed on each MAS. See http://support.microsoft.com/kb/968930.

The following software is available during the migration:

- MAPI/CDO v6.5.8190 or later.
- Additional components as required, such as Microsoft Management Console 3.0 and .NET 3.5 SP1.

For additional information about downloading Modular Messaging Service Packs and patches, see Appendix E: Updating Modular Messaging software on page 303 software.

These instructions assume that when you begin the migration:

- Modular Messaging MASs are using Exchange 2003 or Exchange 2007 servers as peer mail servers.
- All Modular Messaging user Exchange mailboxes in the existing VMD are located on Exchange 2003 or 2007 servers.
- There are no Exchange 5.5 servers in the environment.

Changing the monitor mode

When Modular Messaging is first installed, it is configured to create system mailboxes on every Exchange server that hosts an enabled subscriber mailbox. Avaya recommends that you do not disable this functionality. But if you need to disable, then you will need to reenable the functionality because it may be required during a migration exercise.

To reenable, complete the following steps:

1. On a MAS, launch the Voice Mail System Configuration program.
2. Under the VMD name, double-click **Messaging**.
3. On the **Messaging** window **Configuration** tab, ensure that the Monitor new servers check box is selected.
4. Click **OK** to save the change and close the **Messaging** window.
5. Close the **VMSC** window.

Removing the fail over peers

Any fail over peers that have been configured need to be removed from the configuration of each MAS server. This is to ensure that the migration will complete and create the correct number of monitor mailboxes for the new Exchange servers.

To remove the fail over peers, complete the following steps:

1. On a MAS, launch the Voice Mail System Configuration program.
2. Under **Messaging Application servers**, expand the selection.
3. For each MAS listed, double-click **Messaging** and then select the **Advanced** tab.
4. If any Exchange servers are listed in the **Fail Over Peers** entry, remove them.
5. Ensure this process is carried out for each MAS.

Preparing Exchange 2010

To configure an Exchange 2010 server to function as a Modular Messaging peer or as a non-peer Exchange server, you need to perform the following tasks:

Note:

The customer account name used in this appendix is **mmacct**. In the commands and examples below, substitute this name with the correct customer account for the Modular Messaging implementation. If there is more than one account listed in the Service Account group created for Modular Messaging, you should rerun each command for each of the accounts.

Note:

To complete many of the steps below, you require a higher permissions level than what is typically available to an implementation engineer. Most steps will also require access to the Exchange Management Shell for Exchange 2010, which is not available on the MAS. You can complete this section at any time prior to integrating Modular Messaging with Exchange 2010.

- **Set permissions for the service account:**

  The service account group requires additional security groups added to it. The following table lists the security groups that you need to add depending on the original Exchange server level:

Migrating from Exchange 2003	Migrating from Exchange 2007
Recipient Management Public Folder Management	Recipient Management Public Folder Management

- **Enable remote scripting:**

  Exchange 2010 supports remote administration using Remote PowerShell, but only PowerShell 2.0 supports this feature. By default, remote scripting is disabled for all users. You must enable remote scripting for the service account in order for it to automatically create Modular Messaging specific system accounts and associated mailboxes. This is because the Exchange Management Powershell Snap-in cannot be used on the MAS.

  To enable remote scripting for the service account, run the following command on the Exchange management shell for Exchange 2010.

  ```
  Set-User mmacct -RemotePowerShellEnabled $True
  ```

- **Create Exchange Public Folders:**

  During the installation of Exchange 2010, customers can choose whether or not Public Folders should be available. However, when using MAPI/CDO, public folders are required on the server running Exchange 2010.

  If the public folders are not configured, then perform the following steps to create a public folders database:

  - Open the Exchange Management Console for Exchange 2010.
  - Navigate to **Microsoft Exchange** > **Microsoft Exchange On-Premises** > **Organization Configuration** > **Mailbox** from the left pane of the Exchange Management Console.
  - In the right pane of the Exchange Management Console, click **Database management**.
  - From the list of actions, click **New Public Folder Database**.
  - Follow the prompts to create the public folder database and then mount it.

- **Configure the Throttling policy:**

  Exchange 2010 uses client throttling policies to track the bandwidth that each Microsoft Exchange user consumes and to enforce bandwidth limits. Exchange administrators can use throttling policies to control the resources that can be used by a user. Since Modular Messaging runs under a service account and performs different interactions with Exchange on behalf of end users, the service account must bypass the throttling policies imposed by Exchange 2010. Service Pack 1 for Exchange 2010 includes additional methods for accomplishing that are not available in the GA version.

  To configure the throttling policy for the service account, run the following sequence of commands on the Exchange management shell for Exchange 2010:

  a. Create a new Throttling policy using the following command:

  ```
  "New-ThrottlingPolicy -name"Avaya_MM_ThrottlingPolicy"
    -RCAPercentTimeInAD $null -RCAPercentTimeInCAS $null
    -RCAPercentTimeInMailboxRPC $null –RCAMaxConcurrency $null"
  ```

  b. Attach the newly created throttling policy to the service account:

  ```
  Set-ThrottlingPolicyAssociation -Identity mmacct
    -ThrottlingPolicy "Avaya_MM_ThrottlingPolicy"
  ```

- **Create the Management role:**

  Microsoft Exchange 2010 introduces a Role Based Access Control permissions model. Since the service account requires permission to act on behalf of end users, a new Management Role is required. Use the following command on the Exchange management shell for Exchange 2010 to create the required role:

  ```
  New-ManagementRoleAssignment -Name "Avaya_MM_ImpersonationRole"
    -Role ApplicationImpersonation -User mmacct
  ```

- **Configure NSPI for Windows Server 2008 domain controllers:**

  With Microsoft Windows Server 2008, the number of NSPI connections from an individual user is limited to 50. An NSPI connection is required for each MAPI logon, and if a user limit, is reached then that log-on attempt fails. In Modular Messaging, the service account performs all the logons for all the mailboxes, so this limit is too small. You must increase this limit on every Windows Server 2008 Domain Controller that Exchange may interact with. For more information on this topic, see the Modular Messaging Concepts and Planning Guide for Release 5.2.

  For more details regarding NSPI connections and how to set the connection limit see the Microsoft Knowledge Base article, http://support.microsoft.com/kb/949469.

  Note:

  Introduction of Exchange 2010 does not increase the NSPI demands, so if the NSPI limit was set when Windows 2008 was introduced, no further changes are required.

- **Configuring CAS servers to allow remote PowerShell using "Negotiate" Authentication mode:**

  Exchange Management Tools for Exchange 2010 are not available in the 32bit version, so you should perform the operations that require Exchange Management Tools using Remote PowerShell from the MAS server.

  Remote PowerShell uses Kerberos as a default authentication mechanism. To enable remote PowerShell to use "Negotiate" authentication mechanism, perform the following steps on each of the CAS servers.

  1. Open **IIS Services Manager**.
  2. Navigate to the **Default Web Site**.
  3. Navigate to the **Powershell virtual** directory.
  4. Double-click **SSL Settings** to open the **SSL settings** page.
  5. Clear the **Require SSL** check box for Powershell virtual directory and click **Apply** in the **Actions** pane to apply the new settings.
  6. Close **IIS Services Manager**.
  7. Click **Start**, and then click **All Programs**.
  8. Click **Accessories**, and then click **Command Prompt**.
  9. At the Command Prompt, type ***cd %windir%\system32\inetsrv***, and then press **Enter**.
  10. At the Command Prompt run the following commands.

```
appcmd set config "Default Web Site/PowerShell"
  -section:system.webServer/security/authentication/
  windowsAuthentication /enabled:"True" /commit:apphost

appcmd set config "Default Web Site/PowerShell"
  -section:system.webServer/security/authentication/
```

```
windowsAuthentication /+"providers.[value='Negotiate']" /
commit:apphost

appcmd set config "Default Web Site/PowerShell"
-section:system.webServer/security/authentication/
windowsAuthentication /+"providers.[value='NTLM']" /
commit:apphost

appcmd set config "Default Web Site/PowerShell"
-section:system.webServer/security/authentication/
windowsAuthentication /
+"providers.[value='Negotiate:Kerberos']" /commit:apphost
```

Note:

In some cases, these commands may result in an error message, such as "Cannot add duplicate collection entry of type 'add' with unique key attribute," and so on. This error is caused because the attribute has already been set and does not need to be updated. Using the 'List' command can display the current settings. For example,

```
appcmd list Config "Default Web Site/Powershell"
-section:system.webServer/security/authentication/
windowsAuthentication."
```

- **Ensure that the NTLM compatibility level is set correctly:**

  Modular Messaging requires that the NTLM compatibility level is set to allow clients to only use NTLM v2 authentication. On each MAS, manually set the following registry value to a data value of 3. The default is 2.

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
  lmcompatibilitylevel
  ```

Migrating the Peer Exchange server to Exchange 2010

Use the instructions in this section to migrate an existing Modular Messaging system from Exchange 2003 or Exchange 2007 Peer Exchange servers to Exchange 2010 Peer Exchange servers.

Note:

The VMD Host is typically the Peer Exchange Server associated with the first MAS server that was installed in the VMD. This is the Exchange server that currently hosts the VMD mailbox object.

CAUTION:

Neither Exchange 2007 nor Exchange 2010 supports Octel Analog Networking. To retain use of this feature, the VMD Host must remain as an Exchange 2003 server.

Preparation

Before you begin, ensure the following:

- Modular Messaging is updated with Release 5.2 Service Pack 6 or later.
- Exchange 2010 server is updated with Service Pack 1 or later.
- All steps pertaining to Exchange 2010 listed on Preparing Exchange 2010 on page 374 are performed.

Note:

An Exchange administrator may be required to perform these tasks.

Changing the Peer Exchange server for a MAS

Once the Exchange 2010 configuration is complete, complete the following steps for each MAS in the VMD. Perform the steps on each MAS separately and test each before proceeding to the next. It is not necessary to move all the MASs at the same time.

1. Install the updated MAPI/CDO on the MAS. See MAPI/CDO installation on page 379.
2. Reassign the Peer Exchange server in VMSC, See Reassigning the Peer Exchange server for a MAS on page 380.
3. Relocate the VMD mailbox to the Exchange 2010 server. See Relocating the VMD mailbox on page 381.

   Important:

   Perform this step only once.

   Important:

   Before moving the VMD mailbox from the Exchange 2003 server, stop all MAS services on the MAS and Supplementary servers.

   Note:

   An Exchange administrator may be required to perform this step
4. Clean up the Modular Messaging System mailboxes. See Clean up the system mailboxes on page 382.

MAPI/CDO installation

When migrating from Exchange 2003 to Exchange 2010, you must first uninstall the Exchange Management Tools from the MAS and then install the MAPI CDO v6.5.8190 or later.

When migrating from Exchange 2007 to Exchange 2010, you must update the MAPI/CDO.

Important:
All Modular Messaging services must all be in a stopped state during this procedure.

Migrating from Exchange 2003 to Exchange 2010

To replace the Exchange Management Tools:

1. Navigate to the ***C:\Avaya_Support\Tools\ServiceControl*** directory.
2. Double-click the ***StopMMServices.exe*** file to stop all services on the MAS.
3. Click **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.
4. In the **Add or Remove Programs** window, select **Microsoft Exchange** and click **Change/Remove**.
5. On the **Microsoft Exchange Installation** wizard, click **Next** to see the list of Installed components.
6. Under the **Action** column of the components, select **Change** for **Microsoft Exchange** root component.
7. Under the **Action** column of the components, select **Remove** for **Microsoft Exchange System Management Tools**.
8. Click **Next** and then confirm the change by clicking **Next** again.
9. Click **Finish** to close the **Microsoft Exchange Installation** wizard.
10. In the **Add or Remove Programs** window, select **Microsoft Exchange** and click **Change/Remove**.
11. On the **Microsoft Exchange Installation** wizard, click **Next** to see the list of Installed components.
12. Under the **Action** column of the components, select **Custom** for **Microsoft Exchange** root component.
13. Make sure that the **Action** column against **Microsoft Exchange Messaging and Collaboration Services** shows **"..."**. If not, select **None** from the Microsoft Exchange Messaging and Collaboration Services list.

14. Make sure that the **Action** column against **Microsoft Exchange System Management Tools** shows **"..."**. If not, select **None** from the **Microsoft Exchange System Management Tools** list.
15. Click **Next** and then confirm the change by clicking **Next** again.
16. .Click **Finish** to complete the uninstallation.
17. Install the MAPI CDO v6.5.8190 or later.
18. (Optional) Sometimes MAPI/CDO installation does not register CDO.dll that is commonly located at ***C:\Program Files\ExchangeMapi*** folder. To manually register the CDO.dll, run the following command:

    ```
    regsvr32 C:\Program Files\ExchangeMapi\CDO.dll
    ```

19. Restart the system.

Migrating from Exchange 2007 to Exchange 2010

To update the MAPI/CDO:

Note:

Do not uninstall the Exchange 2007 Management Tools.

1. Run the command ***tasklist.exe /m exmapi32.dll*** to ensure that MAPI is not in use. If there is any, stop it.
2. Uninstall the existing MAPI CDO using **Settings** > **Control Panel** > **Add or Remove Programs**.
3. Delete or rename the file MAPISVC.INF in the ***C:\Windows\System32*** directory.
4. Install MAPI CDO v6.5.8190 or later.
5. (Optional) Sometimes the MAPI/CDO installation does not register CDO.dll that is commonly located at ***C:\Program Files\ExchangeMapi*** folder. To manually register the CDO.dll, run the following command.

   ```
   regsvr32 C:\Program Files\ExchangeMapi\CDO.dll
   ```

6. Restart the system.

Reassigning the Peer Exchange server for a MAS

Use the Voice Mail System Configuration program to change the Peer Exchange server for the MAS to the Exchange 2010 mail server:

1. On the MAS, launch the Voice Mail System Configuration program.
2. Expand **Message Application Servers** and the name of the MAS required.
3. Under the MAS name, double-click **Messaging**.

4. On the **Messaging** window **General** tab in the **Mail Server Name** field, enter the name of the Exchange 2010 peer mail server. This will be the NetBIOS name of the CAS Array that has been defined for the site, alternatively the NetBIOS name of the CAS server (if only one exists) can be entered.
5. Click **OK** to save the change and close the **Messaging** window.
6. Close the **VMSC** window.

   The system displays the following message:

   ```
   You have changed the peer Microsoft Exchange Server. It is
     recommended that you move the External Caller Mailbox to the new
     Server.
   ```

7. Click **OK**.

   The system displays the following message:

   ```
   You must stop & restart MAS Voice Server service for your changes
     to take effect.
   ```

8. Click **OK**.

Relocating the VMD mailbox

You need to relocate the VMD mailbox only once per VMD. You may require the assistance of an Exchange Administrator for this. You should perform the following steps using the Exchange Management Console.

CAUTION:

Before moving the VMD mailbox from the Exchange 2003 server, stop all MAS services on all MAS and Supplementary servers.

1. In the left panel of the Exchange Management Console, select **Recipient Configuration**.
2. In the centre panel, select the VMD mailbox.

   Note:

   The VMD mailbox is named ***OctelVMD{….}{Name of Voice mail Domain}***.
3. In the right panel, click **New Local Move Request**.
4. In the **New Local Move Request** window, browse to the target mailbox database, that is, the Exchange 2010 database.
5. Click **Next** and follow the prompts to complete the move settings.
6. Click **Move Request** in the left pane to verify the status of the moved mailbox.

Clean up the system mailboxes

Modular Messaging creates system mailboxes (External Caller) on each Exchange server to allow it to monitor the availability of the server and to facilitate Peer Fail over. After changing the Peer Exchange server to Exchange 2010, the system mailbox is still hosted on the Exchange 2007 or Exchange 2003 server. To ensure Modular Messaging is monitoring the correct server, you must move the system mailbox. In addition, you also need to relocate the Fax mailbox.

Removing the Peer Exchange system mailbox

You need to delete the original External Caller mailbox and the associated account to allow the software to automatically create a new mailbox on the Exchange 2010 server.

Note:

You can configure Modular Messaging so it does not automatically create new system mailboxes when a new Exchange server is discovered. If required, follow the steps in the section Changing the monitor mode on page 372 to reenable the automatic creation of the External Caller mailbox.

1. Perform one of the following:
   - For Exchange 2003: Click **Start** > **Programs** > **Microsoft Exchange** > **Active Directory Users and Computers**.
   - For Exchange 2007: Click **Start** > **Programs** > **Administrative Tool** > **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** window, highlight the Windows domain used for Modular Messaging.
3. Select **View** and then select **Advanced Features**.
4. In the right pane, double-click **Octel**.
5. In the right pane, locate the External Caller for the MAS that is being upgraded.

   Note:

   The External Caller mailbox is named **External Caller (NetBIOS Name of MAS)**. Do not touch the mailboxes that are named **External Caller (NetBIOS Name of Exchange)**.
6. Right-click on the account that was determined in the above step.
7. Choose **Delete** from the menu.

Continuing with the migration

Now that MAPI/CDO has been upgraded, the VMD has been moved, and the existing monitor mailboxes have been cleaned up, the rest of the migration can be completed.

Creating the non-peer Exchange 2003 system mailbox

Modular Messaging cannot automatically recreate a system mailbox on an Exchange 2003 server. If the original Peer Exchange server was Exchange 2003, complete the following steps to create the non-peer Exchange monitor mailbox:

1. Copy the file ***C:\Avaya_Support\Exchange2007Migration\Add-Monitor-Mbx.exe*** from the MAS to a computer that is running the Exchange 2003 System Management Tools.

   Note:

   This can be an Exchange 2003 server running the Exchange 2003 System Management Tools, or a computer with the Exchange 2003 System Management Tools that is used to administer the Exchange servers.

2. Click **Start** > **Run**, enter **cmd**, and click **OK**.
3. In the command window, enter the following:

   ```
   Add-Monitor-Mbx <Exchange server> <peer directory server> <Octel
     container>
   ```

where,

<Exchange server> is the name of the non-peer Exchange 2003 server you want to monitor.

<peer directory server> is the peer directory server used by the MASs.

<Octel container> is an optional entry that is not required if you are using the default Octel container location. Enter the location of the Octel container if you are not using the default location. For example, *cn=octel,cn=avaya,DC=ncis,DC=local.*

Note:

It is imperative that any remaining Exchange 2003 servers that have or are likely to have MM enabled subscribers on them are configured with monitor mailboxes. Otherwise, Modular Messaging will attempt to automatically create them, which will fail and could cause the system to become unresponsive.

Moving the Fax system mailbox

You need to move the fax system mailbox only once per VMD. For this, you may require the assistance of an Exchange Administrator. You should perform these steps using the Exchange Management Console.

Important:
Before moving the Fax system mailbox from Exchange 2003 server, stop all MAS services on all MAS and Supplementary servers.

1. In the left panel of the Exchange Management Console, select **Recipient Configuration**.
2. In the centre panel, select the Fax system mailbox.

   Note:
   The Fax system mailbox is named **FAX {Name of Voice mail domain}{…}**.
3. In the right panel, click **New Local Move Request**.
4. In the **New Local Move Request** window, browse to the target mailbox database, that is, the Exchange 2010 database.
5. Click **Next** and follow the prompts to complete the move settings.
6. Click **Move Request** in the left pane to verify the status of the moved mailbox.

Moving Subscriber Mailboxes to Exchange 2010

Before starting this procedure, complete all the Installation prerequisites on page 372 and perform the steps listed in Preparing Exchange 2010 on page 374 before proceeding.

To move Modular Messaging enabled Exchange mailboxes to an Exchange 2010 server:

1. Click **Start** > **All Programs** > **Microsoft Exchange Server 2010** > **Exchange Management Console**.
2. In the left panel, select **Recipient Configuration**.
3. In the centre panel, select the mailboxes that you want to move.
4. In the right panel, click **New Local Move Request**.
5. In the **New Local Move Request** window, browse to the target mailbox database, that is, Exchange 2010 database.
6. Click **Next** and follow the prompts to complete the move settings.
7. Click **Move Request** in the left pane to verify the status of the moved mailboxes.
8. On the MAS, wait for the 1027 application event to happen in the event viewer.
9. Test the functionality of the moved mailbox using the telephone user interface (TUI) and client software.

When you move the first subscriber to a new Exchange 2010 server, the monitor mailbox is created automatically on that Exchange server. You can also configure Modular Messaging so that it does not monitor new Exchange servers, in which case this system mailbox is not be created. If the system is configured this way, then perform the steps in the section Changing the monitor mode on page 372 to reenable the automatic creation of the External Caller mailbox.

Note:

You can also use the Exchange Shell move_mailbox command to move mailboxes, or the Exchange Shell script move_mailbox command to bulk move mailboxes. For additional information, see your Microsoft Exchange documentation.

Finishing off

After relocating the VMD and other system mailboxes to the Exchange 2010 server, you can restart and test the Modular Messaging software. To do this:

1. Restart all services by running the *serverrecovery.vbs* script.
2. Verify that the correct services are running on the MAS.
3. Rebuild the FEDB.

After moving all required MASs to the Exchange 2010 peer mail server, perform a complete DCT analysis of the supplementary server and all MASs. All MASs, the supplementary server if present, and the Exchange message store must be running. For more information, see: Using the DCT to collect information from an MAS on page 130 for an Avaya MAS and Using the DCT to collect information from an MAS on page 152 for a customer-provided MAS.

Appendix N: Diminished Permissions for Microsoft Exchange 2003 and Exchange 2007

Previously, the installation of Modular Messaging with Exchange 2003/2007 required the use of distinctive permissions to allow the Modular Messaging (MM) services full access to the corporate Active Directory (AD) Forest of the customer network. These high-level permissions enabled MM to read and modify attributes within the Forest. As part of the installation, membership of the group known as 'builtin\Administrators' is granted to MM. This-high level group within AD allows full access to most of the forest, and each of the Domains below. Because of some security implications, it is beneficial for Avaya and our customers to be able to use restrictive permissions that allowed MM to function correctly, but limit its incursion in to the customers' network.

This appendix is an alternative version of Chapter 2: Preparing to install Modular Messaging software on page 9, which has been redesigned and refreshed and take into account the changes that have occurred to Microsoft Exchange.

This appendix describes how to set up Modular Messaging accounts on the directory server, and how to prepare the directory server to support the Modular Messaging software.The steps in this appendix must be completed by the directory server administrator or other authorized customer personnel before a technician can install Modular Messaging software on the first MAS in the system.

This appendix includes the following topics:

- Overview on page 387
- Setting up Modular Messaging accounts on page 388
- Creating MAS computer accounts on page 402
- Updating the Active Directory and data schema on page 403

Overview

The following is an overview of the system preparation steps discussed in this appendix:

1. For all installations, you must create a Modular Messaging security group, customer accounts and technical support accounts on the directory server, and then add the correct permissions for each account.
2. Depending on local requirements, you must create computer accounts for each MAS in the Active Directory and set up each MAS to allow remote access by technical support staff.
3. You must update the data schema before you install any Modular Messaging software on any MAS in the domain.

Note:

This procedure described in this appendix can be performed only on a computer that is running the Windows Server 2003 or Windows Server 2008 operating system.

Note:

To log on to the directory server, you must use an account that has permission to do Active Directory and data schema administration. This is usually the Windows domain administrator account. The account must have both Domain Admin and Schema Admin rights.

CAUTION:

If you have added Active Directory Extensions, you must reboot the directory server after you install the Modular Messaging software. Schedule down time for the directory server before performing the tasks described in Updating the Active Directory and data schema on page 403.

All servers must meet the requirements listed in the *Avaya Modular Messaging Concepts and Planning Guide*. Review this document to verify that all Exchange servers, directory servers, MASs, and client machines are ready to support Modular Messaging software.

To successfully set up the Windows system to support the Modular Messaging software, you need:

- Access to the *Avaya Modular Messaging Messaging Application Server Software* media.
- A completed copy of the relevant planning forms including:
  - The Corporate network planning form (MAS#1 to MAS#3) showing the NetBIOS name of each MAS, the default (or primary) peer Exchange server, the directory server, and the Windows domain.
  - The Modular Messaging log-on accounts form showing the customer-specified Modular Messaging account names and passwords.
  - Switch and messaging information showing the test subscribers and telephone user interfaces required to test the Modular Messaging software.

Setting up Modular Messaging accounts

You must create two Windows domain user accounts on the directory server to support Modular Messaging, and you must assign sufficient permissions to the accounts.

- Create a customer account to install and administer the Modular Messaging software.

Note:

In pre 3.0 releases this account was referred to as the service account.

- Create a technical support account to allow remote support staff to access and administer the Modular Messaging system.

At this time you can also optionally create a test subscriber account for each TUI that will be used at this site. The test subscriber accounts are required to support acceptance testing after configure the MAS. For more information about creating accounts, see the Microsoft Windows documentation.

Creating Modular Messaging customer and technical support accounts

To prepare for creating customer and technical support accounts, complete the following steps:

1. Log on to the Active Directory server using an account that has privileges to create new user accounts, such as *administrator*.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** dialog box, expand the directory for the Windows domain you intend to use for Modular Messaging.

Creating the Modular Messaging customer account

To create the Modular Messaging customer account, you must first create a new security group for the account and then create the customer account and assign appropriate permissions.

Creating the Modular Messaging customer account group

Create a new security group that will give the Modular Messaging customer account the appropriate permissions.

1. In the left pane, right-click **Users** > **New** > **Group**.
2. In the **New Object - Group** dialog box, create a new security group as follows:
   a. Choose an appropriate name, such as MM Service Permissions.
   b. Select the group scope appropriate for this site.
   c. Select group type **Security**. Click **Next**.
   d. On the next screen, do not create a mailbox (clear the check box if it is selected). Click **Next**.
   e. Click **Finish**.

Creating the Modular Messaging customer account

Create a new account for installing and administering the Modular Messaging software (this is the Modular Messaging customer account).

1. In the left pane, right-click **Users** > **New** > **User**.
2. In the **New Object - User** dialog box, create a new Modular Messaging customer account using a secure log-on name.
   a. First name: Customer
   b. Last name: Account
   c. User logon name: *customer-provided,* such as *mmacct*.

   Note:

   Ensure that you are satisfied with the Modular Messaging account names and passwords that you choose now. They are not easy to change later.

   d. Click **Next**.
   e. Enter and confirm the password.

   Note:

   Passwords for Modular Messaging accounts must be at least eight characters long. Do not create passwords composed of easily guessed words or numeric combinations, including sequential or repeated numbers. You must use a combination of at least three of the following character types: uppercase and lowercase letters, numbers, and special characters or symbols.

   f. Select **Password never expires**.

   Note:

   Contact the software provider for the procedure to change the password for a Modular Messaging customer account.

   g. Click **Next**.
   h. On the following page, clear the **Create an Exchange mailbox** check box.

   Note:

   You do not need to create an Exchange mailbox for a Modular Messaging customer account.

   i. Click **Next**.
   j. When the summary is displayed, click **Finish**.
3. In the right pane, locate the new account and double-click it.
4. In the **Properties** dialog box, click the **Member Of** tab.
   a. Click **Add**.

b. In the **Select Groups** dialog box, add the Modular Messaging customer account security group that you just created, such as MM Service Permissions.

c. Click **OK** to close the **Select Groups** dialog box.

5. Click **OK** to close the **Properties** dialog box.
6. To assign permissions to the Modular Messaging customer account, assign permissions to the customer account group.

Creating the Modular Messaging technical support account

Create a new account to allow remote support staff to access and administer the Modular Messaging system. For example:

1. In the left pane, right-click **Users** > **New** > **User**.
2. In the **New Object - User** dialog box, create a new Modular Messaging remote access account using a secure log-on name.

   a. **First name**: Support

   b. **Last name**: Account

   c. **User logon name**: *customer-provided,* such as *techacct*.

   d. Click **Next**.

   e. Enter and confirm the password.

   f. Select **Password never expires**.

   Note:

   If you ever change the password for the remote access account, be sure to notify the appropriate technical support organization.

   g. Click **Next**.

   h. On the following page, clear the **Create an Exchange mailbox** check box.

   i. Click **Next**.

   j. When the summary is displayed, click **Finish**.
3. In the right pane, double-click the name of the new account.
4. In the **Properties** dialog box, click the **Member Of** tab.
5. Verify that the **Domain Users** entry is present. If the Domain Users entry is missing:

   a. Click **Add**.

   b. In the **Select Groups** dialog box, add **Domain Users** to this account.

   c. Click **OK** to close the **Select Groups** dialog box.
6. Click **OK** to close the **Properties** dialog box.

Creating test subscriber accounts

Create at least one new test subscriber account for each telephone user interface (TUI) to be used at this site. The test subscriber accounts will be used for acceptance testing later in the installation. You may need to create up to three accounts, one for the MM Aria telephone user interface (TUI), one for the MM AUDIX TUI, and one for the MM Serenade TUI. For example:

1. In the left pane, right-click **Users > New** > **User**.
2. In the **New Object - User** dialog box, create a new account, such as:
   a. **First name**: *Aria Test*
   b. **Last name**: *Subscriber*
   c. **User logon name**: *customer-provided,* such as *testsub1*.
   d. Click **Next**.
   e. Enter and confirm the password for the account (*customer-provided*).
   f. Set up other parameters as required for this site.
   g. Click **Next**.
   h. On the third page, verify that **Create an Exchange mailbox** is selected.
   i. Select the required **Server** (Exchange organization) and **Mailbox Store** (Exchange server).
   j. Click **Next**.
   k. When the summary is displayed, click **Finish**.

   A new account is added to the list in the right pane.

   Note:

   The extension for the test subscriber must be administered on the PBX by the appropriate party.
3. Repeat Step 1 and Step 2 to set up test subscribers for AUDIX and Serenade if required for this site.
4. Close the **Active Directory** dialog box.
5. Assign Modular Messaging characteristics to this account after the Modular Messaging software is installed. See Adding a test subscriber on page 108.

Assigning permissions to the customer account group

Use the steps in this section to assign permissions to the Modular Messaging customer account by assigning permissions to the customer account group you created in Creating the Modular Messaging customer account on page 389. You must assign sufficient permissions to the group

for the customer account to function. For details of permission requirements, see Appendix K: Administrator reference on page 351.

To assign permissions to the group:

1. Edit the registry to display the **Security** tab.
2. Add the required permissions.

Editing the registry

By default, the **Security** tab for the Exchange organization container and some of the key subcontainers are not visible using Exchange System Manager or Active Directory Sites and Services. The following registry change enables the **Security** tab at all levels within the Microsoft Exchange container.

To update the registry:

1. Log on as the Microsoft Exchange administrator.
2. Click **Start** > **Run**.
3. In the **Run** dialog box **Open** field, type **regedit** and press **Enter**.
4. In the **Registry Editor** dialog box, locate the following key:

   HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin
5. Right-click **ExAdmin** and select **New** > **DWORD Value**.
6. Double-click the **ShowSecurityPage** value.
7. In the **Edit DWORD Value** dialog box, set the Value data to **1**.
8. Click **OK** to close this dialog box.
9. Click the **Registry Editor** dialog box.

Adding permissions

Use **Active Directory Sites and Services** to add the required permissions. The permissions listed in Step 7 are the absolute minimum required for the Modular Messaging software to function. For convenience, all the properties should be created at the Exchange Organization level. You can apply them at a level lower down the tree if required, but this might affect your ability to manage Modular Messaging using Exchange System Manager.

To assign permissions to the Modular Messaging customer account:

1. Log on to the Active Directory server using an account, such as *administrator*, that has privileges to assign permissions to accounts.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Sites and Services**.
3. In the left pane, select **Active Directory Sites and Services**.

4. From the **View** menu, select **Show Services Node**. The menu item shows a check mark after you select it.
5. In the left pane:
   a. Expand **Services**.
   b. Expand **Microsoft Exchange**.
   c. Locate the appropriate *Exchange Organization* object that Modular Messaging will connect to.
   d. Right-click this object and select **Properties**.
6. In the **Properties** dialog box, click the **Security** tab. This tab is visible only if you edited the registry as directed in the previous procedure.
   a. Click **Add**.
   b. In the **Select Users, Computers, and Groups** dialog box, add the Modular Messaging customer account group, such as MM Service Permissions.
   c. Click **OK** to close this dialog box.
7. Under **Permissions** for the group, **Allow** the permissions listed below. Clear any check boxes that do not apply. For details on these permission requirements, see Appendix K: Administrator reference on page 351.

   Note:

   You may find it easier to verify the permissions by working from the bottom of the list to the top.

   - Read
   - Execute
   - Read permissions
   - Create children
   - List contents
   - Read properties
   - Write properties
   - Administer information store
   - Create named properties in the information store
   - View information store status
   - Receive As
   - Send As
   - View information store status (only with Exchange 2007)
   - Read all properties (only with Exchange 2007)

- Write all properties (only with Exchange 2007)
- Create all child objects (only with Exchange 2007)

8. Click **Apply** to verify the settings.
9. Click **OK** to close this dialog box.
10. Close the **Active Directory Sites and Services** dialog box.
11. Wait 10 minutes for the directory cache to expire.

Manually create the VMD container

Important:

In previous documentation, the Octel container could either be automatically created or manually created. The permissions outlined in this appendix prevent the container from being automatically created. Therefore, you must create the container manually using the following procedure. Moreover, only a domain administrator has the access to create items within the Active Directory Forest.

To use this procedure, you must install ADSIEdit. ADSIEdit is a Microsoft Management Console (MMC) snap-in available as part of Microsoft Windows Server 2003 and Microsoft Windows Advanced Server 2003 Support Tools.

In Windows 2008, ADSIedit is part of the Active Directory Domain Controller Tools feature. To add ADSIedit:

1. In **Server Manager**, click **Features**, then click **Add Features** in the right pane.
2. Expand **Remote Server Administration Tools** > **Role Administration Tools** > **Active Directory Domain Services Tools**.
3. Select the **Active Directory Domain Controller Tools** check box.
4. Click **Next**, then click **Install**.

To assign security settings to the VMD container:

1. Run the **ADSIEdit** Windows support tool.
2. Connect to the **Domain NC** of the domain containing the Modular Messaging customer account.
3. Locate the base location for the voice mail domain container.
4. From the **Action** menu, select **New** > **Object** > **Container**.
5. Give the container the value *Octel* and click **Next**, then click **Finish**.

   Note:

   The name of the container is case-sensitive.
6. Right-click the new container and select **Properties**.
7. In the **Properties** dialog box, click the **Security** tab.
8. At the bottom of the page, select **Advanced**.
   a. Click **Add**.
   b. In the **Select Users, Computers, and Groups** dialog box, add the Modular Messaging customer account group, such as *MM Service Permissions*.
   c. Click **OK** to close this dialog box.

d. The Permission Entry form is displayed. Ensure that the **This Object and all child objects** (**This object and all descendant objects** in 2008) check box, next to **Apply onto,** is selected. In Windows 2008, this check box is next to the **Apply to:** field.

e. Select the **Allow** check box next to **Full Control**. This automatically selects every field.

Note:

You must not select the **Apply these permissions to objects and/or containers within this container only** check box.

f. Click **OK** three times to save the settings and return back to the main ADSI screen.

9. Close the **ADSI Edit** dialog box.

Assigning permissions to the root of the Forest

You need to apply specific write permissions to the Active Directory Forest for Modular Messaging to be able to write data to the directory. These write permissions allow users within the AD to become voice mail enabled. In addition, you need to add the Send As permission to allow MM to send messages to users. You need to add both of these security properties at the root of the Forest to allow them to be inherited by all items within the Forest.

1. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
2. Select the root of the Forest, such as Avaya.com, then from the main menu, select **View** > **Advanced Features**.
3. Right-click the root of the Forest again and select **Properties** > **Security**.
4. At the bottom of the page, select **Advanced**.
5. Click **Add**.
6. In the **Select Groups** dialog box, add the Modular Messaging customer account security group that you created, such as *MM Service Permissions*, and then select **OK**.
7. In the Permissions Entry form, select **User Objects** from the drop-down menu next to **Apply onto** (**Apply to:** in Windows 2008).
8. Scroll to the bottom of the page, and select **Allow** next to **Send As**.

Note:

You must not select the **Apply these permissions to objects and/or containers within this container only** check box at the bottom of the page.

9. Select the **Properties** tab, and then select **User Objects** (**Descendant User objects** in Windows 2008) from the drop-down box next to **Apply onto** (**Apply to:** in Windows 2008).
10. Select the **Allow** check box next to **Write Public Information**.

Note:

You must not select the **Apply these permissions to objects and/or containers within this container only** check box.

11. Click **OK** three times to save the settings and return back to the main **Active Directory Users and Computer** screen.

Changing the permissions of the Deleted Objects container

Ownership of the Deleted Objects container and subsequence read access to the MM security account allows MM to monitor objects within specific domains to be read. The procedures for altering the rights of this object are outlined in a Microsoft Knowledge Base article KB892806, available at http://support.microsoft.com/kb/892806/en-us. Essentially, this process involves using the ADAM dsacls utility to first take ownership of the Deleted Objects Container away from the system, and then adding read access to it for members other than those in the Administrators group.

CAUTION:

You must complete this process for each domain within the customers Forest. Failure to do so can result in inconsistencies within the MM front-end database.

The following procedure can only be carried out by a member of the domain administrators group, and assumes that ADAM retail package has been already installed. This command can be run from any server within the target domain. With Windows 2008 ADAM is available if you have the AD DS server role installed. To use dsacls, you must run the dsacls command from an elevated command prompt. To open an elevated command prompt, click Start, right-click Command Prompt, and then click Run as administrator., In this example the target domain is avaya.com.

1. Run the **ADAM Tools** Command Prompt from **Start** > **Programs** > **ADAM**. (In Windows 2008 run a Command prompt as **Administrator**)
2. Type **dsacls “CN=Deleted Objects,DC=avaya,DC=com” /takeownership**.

Note:

The command is case-sensitive.

The system displays the following output:

```
C:\WINDOWS\ADAM>dsacls "CN=Deleted Objects,DC=avaya,DC=com" /takeownership
Owner: AVAYA\Domain Admins
Group: NT AUTHORITY\SYSTEM

Access list:
{This object is protected from inheriting permissions from the parent}
Allow NT AUTHORITY\SYSTEM     SPECIAL ACCESS
                              DELETE
                              READ PERMISSONS
                              WRITE PERMISSIONS
                              CHANGE OWNERSHIP
                              CREATE CHILD
                              DELETE CHILD
                              LIST CONTENTS
                              WRITE SELF
                              WRITE PROPERTY
                              READ PROPERTY
Allow BUILTIN\Administrators  SPECIAL ACCESS
                              LIST CONTENTS
                              READ PROPERTY

The command completed successfully
```

3. To add permission to the MM Service Permissions group, type the following:

   dsacls “CN=Deleted Objects,DC=avaya,DC=com” /g “avaya\MM Service Permissions”:LCRP

Note:

The command is case-sensitive.

The system displays the following output:

```
C:\WINDOWS\ADAM>dsacls "CN=Deleted Objects,DC=avaya,DC=com" /g "avaya\MM
Service Permissions":LCRP
Owner: AVAYA\Domain Admins
Group: NT AUTHORITY\SYSTEM

Access list:
{This object is protected from inheriting permissions from the parent}
Allow NT AUTHORITY\SYSTEM     SPECIAL ACCESS
                              DELETE
                              READ PERMISSONS
                              WRITE PERMISSIONS
                              CHANGE OWNERSHIP
                              CREATE CHILD
                              DELETE CHILD
                              LIST CONTENTS
                              WRITE SELF
                              WRITE PROPERTY
                              READ PROPERTY
Allow BUILTIN\Administrators  SPECIAL ACCESS
                              LIST CONTENTS
                              READ PROPERTY
Allow Avaya\MM Service Permissions    SPECIAL ACCESS
                                      LIST CONTENTS
                                      READ PROPERTY

The command completed successfully
```

You need to complete Step 2 and Step 3 for every domain within the customer's Active Directory Forest.

Allowing *Send As* permissions to protected groups

A background AD process protects the accounts and groups listed below, and all members of these groups. This process periodically checks and applies a specific security descriptor, which is based on the AdminSDHolder object. This means that initially the Send As permission is inherited by users that are members of these groups. However, this permission is later removed and the permissions are reverted back to those configured for the AdminSDHolder object.

The following list contains the names of protected groups and accounts:

- Administrators
- Schema Admins

- Account Operators
- Enterprise Admins
- Server Operators
- Cert Publishers
- Print Operators
- Administrators (Builtin)
- Backup Operators
- Krbtgt (Builtin)
- Domain Admins

Use the Dsacls.exe utility to add the permission to the AdminSDHolder, which will then update all protected groups and their members.

Note:

Only a member of the domain administrator group can perform this procedure.

Note:

The following procedure only needs to be carried out if an account belonging to any of the protected groups listed below is to be Modular Messaging enabled.

1. From the Command prompt, type the following

   substituting dc=Avaya and dc=Com for the customer fully qualified domain name

2. Run the **ADAM Tools** Command Prompt from **Start** > **Programs** > **ADAM**.
3. Type

   dsacls "cn=adminsdholder,cn=system,dc=avaya,dc=com" /G "\MM Security Group:CA;Send As"

   Note:

   This command is case-sensitive.

After the background process completes, it takes at least 1 hour for the adminSDHolder security permissions to replicate to the protected groups and members of those groups.

Creating MAS computer accounts

Before the Modular Messaging software is installed, the domain administrator must create computer accounts for each MAS and define the Modular Messaging customer account as a user that has permission to join the Windows domain. This procedure facilitates remote access setup and Modular Messaging software installation.

For example, to add a new computer account to the Active Directory:

1. Log on to the Active Directory server using an account, such as Administrator, that has privileges to add a computer account to a domain.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** dialog box, expand the directory for the Windows domain that you will use for Modular Messaging.
4. To create a new computer account, right-click **Computers**, and then select **New** > **Computer**.
   a. In the **New Object - Computer** dialog box, type the computer name for the MAS.
   b. Click **Change**.
   c. In the **Select User or Group** dialog box, enter the Modular Messaging customer account, such as mmacct.
   d. Click **OK**. Back on the **New Object –Computer** dialog box, the account is added to the **User or group** field.
   e. Click **Next**.

   CAUTION:
   Do not select **this is a managed computer**.

   f. Click **Next**.
   g. Click **Finish** to close this dialog box.

Updating the Active Directory and data schema

Complete this task only once per Windows Forest, on the directory server domain controller, before installing the Modular Messaging software on any MAS.

The Active Directory must be updated as described in this section.

Note:

You can perform this procedure only on a computer running the Windows Server 2000, Windows Server 2003, or Windows Server 2008 operating system. These components cannot be installed on a workstation operating system.

Note:

To complete this update, you must log on to the directory server using an account that has permission to do Active Directory and data schema administration. This is usually the Windows domain administrator account. The account must have both Domain Admin and Schema Admin rights.

If you are running Windows 2000 or 2003 with Active Directory, you must update the data schema before you install any Modular Messaging software on any MAS in the domain. The schema defines the objects and properties stored in Active Directory, and contains definitions of object attributes. Update the schema only once in the forest.

For details about the changes made to the schema for a Modular Messaging software update, see Appendix K: Administrator reference on page 351.

CAUTION:

If you do not update the schema first when required, the Modular Messaging software does not install correctly. You need to completely remove it and then reinstall it after an Active Directory schema update.

Logging on and preparing to update

It is not possible to update the schema on a Windows Domain Controller that holds the schema operations master role without first allowing the permission. For more information, see the Microsoft knowledge base article KB285172.

Enabling Schema Updates by means of the Registry

To directly edit this registry key, perform the following steps:

1. Click Start > Run.
2. In the **Open** box, type: **regedit** and press **Enter**.

3. Locate and click the following registry key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

4. Find the **Dword** value called **Schema Update Allowed**.
5. Type **1** to enable Schema updates, or **0** (zero) to disable it.
6. Close the **Registry Editor** dialog box.

The schema is updated on the domain controller that holds the schema operations master role.

Updating the Active Directory for Modular Messaging

To update the Active Directory for Modular Messaging:

1. Log on to the directory server using an account that has permission for Domain Administration and Schema Administration.
   - This account is usually the Windows domain administrator account. For an Exchange 2000 or 2003 system, this account requires both Domain Administration and Schema Administration rights.
   - If you are updating the messaging software in a child domain, the account must have Domain Admin rights for both the parent domain and the child domain. If you are updating the Active Directory from the child domain controller, enter the account name in the format: Parent Domain\Domain Admin.
   - If you are using Octel Analog Networking, perform this procedure on the domain controller that is acting as the schema master.
2. To close applications or stop monitoring:
   a. Close the Active Directory Users and Computers application or the Microsoft Exchange Administrator application, depending on the application that is installed to support this version of Exchange.
   b. Close any open windows for other applications.
   c. Stop any monitoring tools that are running, such as antivirus software.

Running the Modular Messaging installation wizard

When all preparations are complete, run the Modular Messaging Installation Wizard as follows:

1. Insert the *Avaya Modular Messaging Messaging Application Server Software* media (disk 1) into the DVD drive of the directory server.

Note:

If the directory server does not contain a DVD drive, you can insert the Avaya Modular Messaging Messaging Application Server Software media into the shared DVD drive of another computer, and then map it as a network drive on this server.

2. Run the Modular Messaging Installation Wizard as follows:
   a. In Windows Explorer, navigate to the DVD drive, such as D:.
   b. Navigate to the **Install directory**.
   c. Double-click the file **Setup.exe**.
3. On the main screen, verify that the **Configuration** drop-down box shows **Microsoft Exchange**.

Updating the Active Directory

To update the Active Directory and data schema (if required) on this computer:

1. Click the plus sign (**+**) to expand the **Active Directory updates** folder.

   Note:

   Do this task only once in the Active Directory Forest.

2. Select the following check boxes to install the appropriate software components to support Modular Messaging:
   - **Enable Modular Messaging***:* Click this box to enable extension data replication among Active Directory servers. This allows Modular Messaging to store subscriber configuration information and support the correct operation of and access to client applications.
   - **Enable Octel Analog Networking***:* If Octel Analog Networking is used at this site, click this box to add the appropriate classes and attributes to the schema. This causes a Modular Messaging Octel Analog Networking tab to appear in the Microsoft Exchange administration program.
   - **Enable User Administratio***n:* Click this box to enable objects that will appear on the Modular Messaging tab in the Active Directory. This allows administrators to use Microsoft Exchange administration to enable Modular Messaging features for users, groups, or contacts.

   Note:

   Although Octel Analog Networking is an optional feature, you might choose to install it at this time in case Octel Analog Networking is ever added to the system. The other schema updates are always required.

3. When all required components are selected, click **Install**.

4. Each component you select causes a Modular Messaging Active Directory installation wizard to run. Complete each wizard as follows:
   a. On the welcome screen, click **Next**.
   b. If prompted, enter the name and password of an account that has both Domain Admin and Schema Admin rights. (For example, *windowsdomain**schemaAdmin* and password.) Click **Next**.
   c. After the Active Directory registration process is complete, click **Next**.
   d. To complete the wizard, click **Finish**.
   e. Repeat Step a through Step d for each occurrence of the wizard.
5. When component installation is complete, click **Close**.

After performing the above procedure, continue with Chapter 3: Adding Exchange extensions for Modular Messaging on page 37.

Index

Numerical

3,x, and 4.0 . . . . . 245, 249

A

about this book xiii
acceptance tests 107, 112, 114, 118
account permissions 351
Active Directory
  adding computer accounts for MAS 31, 402
  assigning permissions 22, 24, 393
  creating required accounts 10, 18, 389
  data schema 33, 355, 403
  Exchange extensions 41
  Modular Messaging tab 37, 39, 40, 41, 355
  setting up remote access 32
  test subscriber 14, 108, 115, 118, 392
  updates 33, 35, 355, 403
administrator reference 351
alarm origination test 105
alarming
  MAS setup 87
  method to use 87
alarming setup 105
alarming telephone number 100
analog boards
  cabling 300
  changing to QSIG 269
  configuring 314
  jumper settings 292, 294, 296
  supported boards 286, 308
  testing 317
  tone file 277, 278, 281, 316
anti-virus software
  disabling 34, 41, 137, 161
  enabling 139, 162
  obtaining and installing 7, 54
ART
  product ID 93
attended backup 119
Audit Service
  configuring 96
  moving service 261
  verifying 106
Avaya MAS
  installation checklist 226
Avaya MAS setup 45
  overview 46

Avaya Modular Messaging Configuration wizard
port board configuration . . . 307
Avaya software updates, *see* software updates

B

backing up the system . . . 119
Belkin KVM switch . . . 128

C

cabling
MAS port boards . . . 300
Call Me - Voice Mail Domain window . . . 257
Call Me Server . . . 94, 257
Caller Applications
back up editable files . . . 129, 152, 177
Caller Applications Editor . . . 119
CAS servers . . . 28, 376
CDO . . . 372
changes from last issue of book . . . xiv
changing DSE or analog to QSIG . . . 269
changing DSE or QSIG to H.323 . . . 270
changing DSE or QSIG to SIP . . . 272
changing from DSE . . . 269
changing H.323 to SIP . . . 274
changing QSIG T1 to QSIG E1 . . . 273
checklist . . . 225
checklist for installing the system . . . 225
checklists
installing new system . . . xv
obtaining . . . 5
upgrades . . . 170, 194
client software packages . . . 254
comment on this book . . . xviii
computer accounts in Active Directory . . . 31
configuration notes . . . 86, 102
configuring VMSC . . . 100
obtaining . . . 4
port boards . . . 277, 309, 318
upgrades . . . 125, 129, 147, 152, 170, 194, 331, 337
configuring an Avaya MAS . . . 45
configuring Messaging Application Servers 99, 101, 102, 258
configuring port boards . . . 102, 301, 307, 309
configuring port groups . . . 258
Configuring System screen . . . 50
configuring the modem . . . 301
configuring the network card . . . 200
configuring the voice mail system . . . 79
contact information . . . xviii
creating a new tone file . . . 277, 278, 281
creating Modular Messaging accounts . . . 10, 388
creating test messages . . . 114
CT bus cable . . . 299
customer account . . . 68, 204
customer responsibility for system security . . . 6
customer-provided equipment
port boards . . . 286
customer-provided MAS
adding accounts to local group . . . 68, 204
adjusting system values . . . 202
installation checklist . . . 230
joining a Windows domain . . . 67, 201
network card . . . 200

D

data schema . . . 403
data schema update . . . 33, 403
DCT
analyze servers . . . 266
collecting data for upgrades . . . 130, 152
Data Collection Tool window . . . 49, 70
data file . . . xv, 170, 194, 266
final handoff of data file . . . 266
help . . . 3
Dialogic Configuration Manager . 277, 278, 311, 312, 314
Dialogic Configuration Manager Properties window 311, 313, 315
Dialogic drivers . . . 136, 159, 299, 301
Dialogic Line Test Application window . . . 317, 318, 319
Dialogic Line Tester program . . . 317
Diminished Permissions . . . 387
directory server . . . 9, 387
disabling Modular Messaging services . . . 255, 264
documentation . . . xvii, 2
library . . . 5
media . . . 5
requirements . . . 3
dsacls utility . . . 18, 19
DSE
changing to H.323 . . . 270
changing to QSIG . . . 269
changing to SIP . . . 272
DVD contents . . . 2

E

E1-QSIG boards
cabling . . . 300
configuring . . . 311
jumper settings . . . 289
plug for unused connector . . . 286
supported boards . . . 286, 308
testing . . . 317
enabling services on the correct server . . . 263, 264
event viewer . . . 82, 101, 103, 317
Exchange 2007
in new VMD . . . 360

installation scenarios . . . 357
migration . . . 363
new installation . . . 358
required Microsoft downloads . . . 47, 170, 194
Exchange 2010 . . . 371
Exchange extensions update . . . 37
Exchange permissions . . . 351, 352
Exchange Recipient Administrators group . . . 11, 351

F

F1 key (help) . . . xviii
Fax - Voice Mail Domain window . . . 261
Fax Sender Server . . . 261
Fax system mailbox . . . 384

H

H.323
changing from DSE or QSIG . . . 270
changing to SIP . . . 274
hardware installation
cabling . . . 300
port board cables . . . 300
port boards . . . 308
preinstallation requirements . . . 287
help using the system . . . xviii
hotfixes to Avaya software . . . 4

I

INADS alarming . . . 99
initial administration for switch and LAN . . . 8
installation
Avaya MAS setup . . . 45
backing up system . . . 119
checklist
checklist for upgrading the system . . . 225
configuring port boards . . . 307
configuring voice mail system . . . 79
creating a new tone file . . . 277
load new operating system . . . 321
testing the system . . . 107
updating Exchange extensions . . . 37
integrated mode test . . . 112
Intel Dialogic Configuration Manager window 137, 160, 280, 281, 284, 311, 312, 314, 315
Intel Dialogic Configuration Manager, *see* Dialogic Configuration Manager
Internet Explorer security update . . . 134, 157
Internet Information Services (IIS), *see also* IIS Admin service . . . 65, 198
IP H.323 integration . . . 285, 307
IP SIP integration . . . 285, 307

J

joining a Windows domain . . . 67, 201

K

KVM switch
showing the correct server . . . 128, 321

L

Languages - Voice Mail Domain window . . . 95
Learn Tones window . . . 279, 282
learning tones . . . 277, 278, 281
license file backup . . . 119
links to other files . . . xvi
loading new MAS software . . . 321
local administrator account . . . 68, 204, 254
logs, changing default location . . . 77

M

Mailbox Monitor Server
configuring Call Me and MWI . . . 257
moving service . . . 257
MAS
installing software updates . . . 346, 348
port groups . . . 258
MAS administration
back up data . . . 221
computer accounts . . . 31
in VMSC . . . 82, 99
load new software . . . 321
preparing the server for service . . . 185
remove software . . . 327
scheduling backups . . . 221
showing the correct server . . . 321
testing port boards . . . 317
MAS port board installation . . . 298
MAS-specific parameters . . . 99
maximum number of supported ports . . . 286
message queuing, installing . . . 65, 156, 198
Message Waiting Indicator - Voice Mail Domain window 95, 258
Message Waiting Indicator (MWI) Server . . . 95
Messaging - Voice Mail Domain window . . . 98
Messaging Application Server Number screen . . . 50
Microsoft Windows SP2 . . . 133, 156
Microsoft Windows updates 7, 66, 67, 133, 140, 156, 164, 186, 199, 217
Migration
checklist . . . 245, 249
from Modular Messaging Release 1.1 . . . 245, 249
overview . . . 169, 172, 195

migration
pre-migration tasks . . . 206
MISCM directory . . . 308
MM Aria interface
acceptance tests . . . 115, 117
MM AUDIX interface
acceptance tests . . . 114, 115, 117
MM Fax Service
configuring . . . 96, 141, 165
moving service . . . 259
MM Messaging Application Server . . . 101, 102
MM Serenade interface
acceptance tests . . . 115, 117
modem installation . . . 301
Modular Messaging accounts . . . 10, 388
Modular Messaging Release 1.1 upgrades . . . 236, 241
Modular Messaging service accounts . . . 68, 204
Modular Messaging services
disable . . . 255, 264
enable . . . 264
moving among servers . . . 257
reset . . . 133, 156
restart . . . 265
start . . . 81
stop . . . 133, 156, 255, 263
verify correct services are started on MAS . . . 265
monitor
showing the correct server . . . 321
Monitor Mode . . . 372
Monitor window . . . 82, 255
moving Modular Messaging services among servers . 257
MWI
configuring . . . 95
moving service . . . 257, 258
port groups . . . 258
testing operation . . . 112

N

network card configuration . . . 200
nonintegrated mode test . . . 114
non-peer monitor mailbox . . . 369
Notify Me . . . 94
NSPI . . . 36, 376

O

Octel Analog Networking . . . 33, 35, 41
offline access feature . . . 98
online help . . . xviii
outcalling test . . . 319

P

passwords
security . . . 6
patches to Avaya software . . . 4, 185, 216
PBX
configuration notes . . . 4, 86, 100, 102, 277, 309
integration . . . 102
PBXpert utility for tones file . . . 277, 281
PBXpert wizard . . . 278, 279
performing acceptance tests . . . 114, 118
permissions
Exchange 2007 permissions . . . 22
remote access . . . 32
send as . . . 17
permissions for customer account . . . 351, 352
planning forms
migration . . . 206
upgrades . . . 170, 194
port boards
configuring . . . 102, 301, 307, 309, 311, 312
connecting cables . . . 300
CPE servers . . . 286
drivers and software . . . 299, 301
enabling . . . 311, 313, 314
errors . . . 317, 319
installation . . . 287, 298
jumper settings . . . 288
ports supported per MAS . . . 286
supported boards . . . 308
testing . . . 313, 317, 319
updating drivers . . . 136, 159
port groups . . . 258
PowerShell script for Exchange 2007 installation . . . 16
preinstallation requirements
LAN and PBX or switch administration . . . 8
security . . . 6
product ID number . . . 93
Protected Groups . . . 400
Public Folders . . . 27, 375

Q

QSIG . . . 269
changing to H.323 . . . 270
changing to SIP . . . 272
QSIG T1 to QSIG E1 . . . 273
QSIG E1
changing from QSIG T1 . . . 273

R

RAS and IAS Servers Properties window . . . 32
RAS IP addresses . . . 128, 151, 206

related resources xvii
remote access account 13, 391
remote access setup 32
remote scripting 27, 374
remote support center xvii
remove MAS software 327
remove test subscribers 118
removing scheduled tasks if you move the Tracing Service 262
required documentation and software 3
restarting messaging service 265
retrieving test messages 112
running Modular Messaging Installation wizard . . . 34, 41

S

scheduled backup 119
scheduled tasks on tracing server 262
schema updates 355
security 6
security patches 7, 67, 140, 164, 186, 199, 217
security tab, displaying 24, 393
Select Computer window 258, 261
send as permission
  description 354
  protected groups and users 18
sending test messages 114
serverrecovery script 136, 159, 265
service accounts
  creating 13, 391
Service Pack updates 4, 185, 216
service patches 66, 133, 156, 199
Serviceability - Voice Mail Domain window 87
set emulation boards
  cabling 300
  configuring 312
  jumper settings 290, 291
  supported boards 286, 308
  testing 317
setting up remote access 32
Shut Down Windows window 322
SIP
  changing from DSE or QSIG 272
  changing from H.323 274
site requirements
  test equipment 7
SNMP
  enabling trap service 88
software
  required for Modular Messaging 3
  requirements 3
software shipped with system 2
software updates
  installing 4, 185, 216
  obtaining 4, 46, 60, 170, 194, 331, 337, 345
Subscriber Administration extensions 38, 40, 355
Subscriber Options package 355
subsequent MAS 141, 165
Supplementary server
  0 port MAS 267
supplementary server
  installing CPE server 285
switch integration
  changing boards during upgrade 269
switch, *see* PBX
Sysprep window 50
system security 6

T

T1-QSIG boards
  cabling 300
  configuring 311
  jumper settings 289
  plug for unused connector 286
  supported boards 286, 308
  testing 317
technical assistance xvii
Telephone User Interface 82
telephones for acceptance testing 7
Telephony Configuration wizard 101
Telephony Interface configuration 102, 258
test equipment 7
test subscriber 15, 392
  remove 118
testing outcalling capability 319
testing port boards 317
testing the system 107
Text-to-Speech (TTS) feature 95
Throttling policy 28, 375
tone file 132, 155
  backup 283
  creating 277, 281
  selecting 315
Tracing Server service
  moving 261
track messaging service startup 82, 101, 103
trademarks xvii
training xviii

U

updating Active Directory and data schema . . . 33, 403
updating Exchange extensions 37
upgrade
  checklist
    checklist for migrating the system
      migration 225
upgrades
  changing DSE or analog to QSIG 269

changing DSE or QSIG to H.323 270
changing DSE or QSIG to SIP 272
changing H.323 to SIP 274
changing QSIG T1 to QSIG E1 273
changing switch integrations 269
checklist 236, 241
client software 142, 166, 254
configuration notes 129, 152
configuring port boards 307
Dialogic drivers 136, 159
Exchange extensions 40, 142, 166
from Modular Messaging Release 1.1 . . . 236, 241
multiple-MAS configuration . . . 127, 150, 173, 196
overview . . . . . xv, xvi, 126, 149
preparing the server for service 185
pre-upgrade tasks 128, 151
requirements 125, 147
supported port boards 308, 310, 312
test subscribers 108
testing port boards 317
verify correct MM services are started 265
USB drive
inserting into server 304
using links in this book xvi

V

verify
alarming setup 105
audit service 106
call handling 104
tracing service operation 105
virtual memory size for MAS 64, 203
virus-checking software 7, 54
VMSC setup
Call Me Server 257
Fax Sender Server 261
Messaging Application Servers 258
MWI Server 258
voice mail domain 82, 94, 257, 262
Voice Mail System Configuration (VMSC) setup 79, 94, 99
Audit Service 96
Call Me Server 94
Languages 95
Message Waiting Indicator Server 95
Messaging Application Servers 99, 101, 102
MM Fax Service 96
Notify Me 94
Offline Access 98
PBXs 102
port boards 102
Serviceability 87, 99
Telephone User Interface 82
Voice Mail System Configuration window 82, 94, 99, 257, 258, 262

W

Windows Components wizard . . . 64, 65, 156, 197, 198
Windows fax service, installing 65, 156, 198
Windows product key 50, 322
Windows Security window 322
Windows services 263
verifying and installing 88
Windows Setup wizard 50
World Wide Web Server, *see* Windows services . 65, 198