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. See 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/Licenselnfo/ (“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 sold by Avaya and used 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 used by End User.

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

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

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

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the "shrinkwrap" or "clickwrap" license accompanying the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya on End User's request (see "Copyright" below for more information).

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). Note 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 through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Use (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, 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 is and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits 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 Européenne) 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
Aria, AUDIX, Avaya, DEFINITY, INTUITY, and Serenade are registered trademarks of Avaya Inc.
COMPAS and Mailbox Manager are trademarks of Avaya Inc.
All non-Avaya trademarks are the property of their respective owners.

Document ordering information:
Avaya Publications Center
For the most current versions of documentation, go to 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 137359.

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** ................................................................. 1
  - Intended audience ....................................................... 1
  - Changes to this book ................................................... 2
**How to use this book** ....................................................... 3
  - Installing a new system ................................................ 3
  - Upgrading a system ...................................................... 3
  - Migrating a system ..................................................... 4
  - Using links in this document ......................................... 4
**Trademarks** ........................................................................ 4
**Related resources** ............................................................. 5
  - User Documentation ....................................................... 5
  - Technical assistance ..................................................... 5
    - Remote support center .............................................. 5
    - Help on the system .................................................. 5
  - Training ........................................................................... 6
  - How to comment on this book ......................................... 6

**Chapter 1: Preinstallation requirements** .............................. 7
  - Software shipped with the system .................................... 8
  - Obtaining the DCT data file ............................................ 9
  - Downloading required software and documentation ............ 9
    - Downloading software updates .................................... 10
    - Downloading configuration notes ................................. 11
    - Downloading the installation and upgrade checklists ....... 11
    - Downloading user documentation ............................... 12
  - Security considerations ................................................ 13
    - On-site security considerations ..................................... 13
      - Password security protection .................................... 13
      - System security protection during installation ............ 13
    - Ongoing system security considerations ....................... 14
  - Test equipment recommendations ..................................... 14
  - Initial switch and LAN administration ............................. 15
    - Initial switch or PBX administration ............................ 15
    - Initial LAN administration ......................................... 15
  - Private Windows domain consideration with MM Fax Sender service .................................................. 16
  - Corporate Windows domain requirements .......................... 16
    - Creating user accounts in the corporate Windows domain .................................................. 17
    - Creating computer accounts in the corporate Windows domain .................................................. 18
    - Adding RAS and IAS permissions to the technical support account .................................................. 19
Chapter 2: Performing initial MSS administration ........................................... 21
  Logging on to the MSS ................................................................. 22
  Adjusting the display settings, if needed ........................................... 23
  Starting the MSS configuration using a DCT data file .......................... 24
Configuring the MSS manually ......................................................... 26
  Setting up network addressing ....................................................... 27
  Setting the time and date ............................................................. 31
  Setting up the MSS local machine .................................................. 32
  Setting up the trusted servers ....................................................... 33
    Adding each MAS as a trusted server ......................................... 33
    Adding the MWI trusted server, if used ..................................... 35
    Adding optional trusted servers .............................................. 36
    Updating the IMAP4 password and the system protocols ................. 37
  Rebooting the MSS ................................................................. 39
Chapter 3: Configuring the Avaya MAS .................................................. 41
  Displaying an MAS from the console ............................................. 42
  Completing MAS configuration prerequisites .................................... 43
    Configuring MASs using an existing DCT data file ......................... 44
  Preparing the new server ........................................................... 47
    Updating Windows Internet Explorer 7 security ........................... 47
    Installing and administering anti-virus software ........................ 48
    Updating Microsoft Windows ..................................................... 49
    Entering RAS IP addresses on each MAS ................................... 50
  Configuring MAS port boards ...................................................... 52
  Configuring the voice mail system ............................................... 53
    Configuring required domain-wide features ............................... 54
      Specifying languages ........................................................... 55
      Verifying that Modular Messaging service has started on MAS#1 ... 55
    Configuring TUI and audio settings on MAS#1 ............................ 56
    Configuring the PBX type on MAS#1 ......................................... 57
    Configuring serviceability settings on MAS#1 ............................ 58
    Obtaining and installing a license on MAS#1 ............................... 60
  Verifying license installation and specifying TTS sessions ................. 62
  Adding the Supplementary server name into the security configuration ... 62
  Entering Product ID for current MAS ............................................ 63
  Configuring specific features as needed ....................................... 64
    Configuring Call Me service ................................................... 65
    Configuring Notify Me .......................................................... 65
Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring MWI service</td>
<td>66</td>
</tr>
<tr>
<td>Configuring MM Audit Service</td>
<td>67</td>
</tr>
<tr>
<td>Configuring the MM Fax Sender server</td>
<td>68</td>
</tr>
<tr>
<td>Configuring languages and multi-lingual TTS</td>
<td>71</td>
</tr>
<tr>
<td>Configuring offline access to messages</td>
<td>73</td>
</tr>
<tr>
<td>Configuring MAS-specific parameters</td>
<td>74</td>
</tr>
<tr>
<td>Configuring Modem Dialout alarming, if used</td>
<td>74</td>
</tr>
<tr>
<td>Configuring port boards and switch integration</td>
<td>75</td>
</tr>
<tr>
<td>Restarting the messaging services</td>
<td>77</td>
</tr>
<tr>
<td>Verifying basic operation of the MAS</td>
<td>80</td>
</tr>
<tr>
<td>Verifying call-handling capability</td>
<td>80</td>
</tr>
<tr>
<td>Verifying alarming setup</td>
<td>81</td>
</tr>
<tr>
<td>Verifying Tracing Service operation</td>
<td>82</td>
</tr>
<tr>
<td>Verifying Audit service</td>
<td>83</td>
</tr>
<tr>
<td>Continuing the installation</td>
<td>83</td>
</tr>
<tr>
<td>Chapter 4: Configuring a customer-provided MAS</td>
<td>85</td>
</tr>
<tr>
<td>CPE MAS configuration prerequisites</td>
<td>86</td>
</tr>
<tr>
<td>Preparing the CPE MAS</td>
<td>87</td>
</tr>
<tr>
<td>Installing Microsoft Windows 2003 R2 operating system</td>
<td>87</td>
</tr>
<tr>
<td>Setting a computer name</td>
<td>87</td>
</tr>
<tr>
<td>Running recommended disk checks</td>
<td>87</td>
</tr>
<tr>
<td>Installing and enabling Microsoft Windows services on CPE MAS</td>
<td>88</td>
</tr>
<tr>
<td>Installing Microsoft Windows services</td>
<td>88</td>
</tr>
<tr>
<td>Enabling Microsoft Windows services</td>
<td>89</td>
</tr>
<tr>
<td>Installing Microsoft Windows updates and security patches</td>
<td>90</td>
</tr>
<tr>
<td>Installing Microsoft Windows 2003 SP2</td>
<td>90</td>
</tr>
<tr>
<td>Adjusting system values</td>
<td>90</td>
</tr>
<tr>
<td>Network connections</td>
<td>92</td>
</tr>
<tr>
<td>Verifying network adapters and bindings</td>
<td>93</td>
</tr>
<tr>
<td>Changing the Power Management settings</td>
<td>93</td>
</tr>
<tr>
<td>Configuring the CPE MAS</td>
<td>95</td>
</tr>
<tr>
<td>Running the Modular Messaging Configuration wizard</td>
<td>95</td>
</tr>
<tr>
<td>Completing the CPE MAS configuration</td>
<td>98</td>
</tr>
<tr>
<td>Entering the RAS IP addresses on CPE MAS</td>
<td>98</td>
</tr>
<tr>
<td>Setting logging location</td>
<td>98</td>
</tr>
<tr>
<td>Installing anti-virus software</td>
<td>99</td>
</tr>
<tr>
<td>Configuring the port boards</td>
<td>99</td>
</tr>
<tr>
<td>Continuing with CPE MAS configuration</td>
<td>100</td>
</tr>
</tbody>
</table>
Chapter 5: Completing initial MSS administration ........................................ 101
  Continuing the MSS configuration using a DCT data file ......................... 102
  Continuing the MSS configuration manually ......................................... 103
    Updating MAS host information ....................................................... 103
      Updating MAS host information in a private Windows domain ............... 103
      Updating MAS host information in a corporate Windows domain .......... 106
  Placing the MSS in a Windows domain .............................................. 108
    Placing the MSS in the private Windows domain ................................ 108
    Placing the MSS in the corporate Windows domain ................................ 109
  Administering classes of service .................................................... 110
    Setting up a cos for required special mailboxes ............................... 110
    Setting up a cos for test subscribers .......................................... 111
  Administering special mailboxes .................................................... 112
    Adding test subscribers .................................................................. 114

Chapter 6: Performing acceptance tests for a new installation .................. 117
  Setting up monitoring tools—optional ................................................ 118
    Using the Operation History Viewer ............................................... 118
    Setting up the port monitor ......................................................... 119
  Running acceptance tests .................................................................... 120
    Leaving a call answer message ....................................................... 120
    Retrieving test messages in integrated mode .................................... 121
    Creating and sending a test message in nonintegrated mode ................ 123
    Testing the outcalling capability .................................................... 124
    Creating and printing a fax message .............................................. 127
  Removing the test subscribers on the MSS .......................................... 128

Chapter 7: Setting up support and making system backups ....................... 129
  Setting up logins and remote access .................................................. 130
    Registering the system in ART ....................................................... 130
      Registering an MSS .................................................................... 130
      Registering an MAS .................................................................... 130
    Administering logins and passwords .............................................. 131
    Setting up the PPP server configuration ......................................... 132
  Setting up alarming on the MSS ........................................................ 133
    Specifying MSS alarm origination ................................................... 133
    Testing alarming origination ......................................................... 135
Using the DCT to analyze the current configuration ........................................ 136
  Copying the DCT data file for backup ......................................................... 138
Backing up the system .................................................................................... 139
  Running backups on each MAS .................................................................. 139
  Setting up and running a backup on the MSS .............................................. 141
Completing the installation ............................................................................ 142
  Installing the client software ..................................................................... 142
  Turning over the system .............................................................................. 143

Chapter 8: Upgrading to Modular Messaging Release 5.0 on S3500-family server .. 145
  Planning for the upgrade from Release 3.x or Release 4.0 ......................... 146
  Upgrade requirements .................................................................................. 148
  Switching the monitor to show the correct server .................................... 149
Performing pre-upgrade tasks ....................................................................... 150
  Preparing for the upgrade .......................................................................... 150
  Preparing for the upgrade on the MAS ....................................................... 151
  Installing the Pre-upgrade and Backup Verification tool ......................... 153
  Running the Pre-upgrade tool ................................................................... 153
  Completing pre-upgrade tasks ................................................................... 155
  Using the DCT to collect information from an MAS ................................. 156
  Collecting DCT data ................................................................................... 156
  Verifying DCT data ....................................................................................... 156
  Busying out ports on each MAS ................................................................. 159
  Checking the spool folder on each MAS ..................................................... 160
  Backing up each MAS .................................................................................. 161
  Backing up the MSS ..................................................................................... 162
  Running the Backup Verification tool ....................................................... 164
Upgrading the MSS from Release 3.x or Release 4.0 ...................................... 166
Upgrading an MAS from Release 3.x or Release 4.0 ...................................... 168
  Logging off all remote logins ..................................................................... 168
  Upgrading overnight ...................................................................................... 168
  Upgrading RealSpeak ................................................................................. 168
    Stopping all MM services ......................................................................... 169
    Uninstalling and re-installing RealSpeak ................................................. 169
    Starting all MM services ......................................................................... 171
  Upgrading Dialogic drivers ........................................................................ 171
  Upgrading the MAS software ..................................................................... 172
  Installing software updates ....................................................................... 175
Completing the upgrade from Release 3.x or Release 4.0 ......................... 176
  Completing the upgrade .............................................................................. 176
## Contents

Converting Supplementary server to run a 0 port MAS on the Supplementary server

Changing switch integration ............................................................ 181  
  Changing from DSE or Analog to QSIG ......................................... 181  
  Changing from DSE or QSIG to H.323 ........................................... 183  
  Changing from DSE or QSIG to SIP .............................................. 184  
  Changing from QSIG T1 to QSIG E1 ............................................ 185  
  Changing from H.323 to SIP. ...................................................... 187  

Moving to the corporate Windows domain after upgrade. .................... 188  
  Preparing to join an upgrade to the corporate Windows domain ........ 189  
  Moving subsequent servers to the corporate Windows domain .......... 190  
    Preparing the system before moving subsequent servers ............. 190  
    Moving subsequent servers. .................................................. 192  
  Moving the MSS to the corporate Windows domain ........................ 194  
  Moving MAS#1 to the corporate Windows domain ......................... 194  
  Completing the move to the corporate Windows domain ................. 196  

Chapter 9: Migrating to Modular Messaging Release 5.0 on S8730-family server .. 201  
  Migration requirements ............................................................ 202  
  Switching the monitor to show the correct server ........................ 203  
  Preparing for the migration ..................................................... 204  
    Performing pre-upgrade tasks ............................................... 205  
      Installing the Pre-upgrade and Backup Verification tool .......... 205  
      Running the Pre-upgrade tool ............................................ 205  
      Completing pre-upgrade tasks .......................................... 206  
      Adding a new server. ...................................................... 206  
  Using the DCT to collect information from an MAS ....................... 206  
    Collecting DCT data .......................................................... 206  
    Verifying DCT data .......................................................... 207  

Migrating MSS and MAS to the S8730-family server ......................... 210  
  Preparing MAS#1 for the migration. ......................................... 211  
    Busying out ports on MAS .................................................. 211  
    Checking the spool folder on each MAS ................................... 211  
  Backing up each MAS ........................................................... 212  
  Backing up the MSS ............................................................ 212  
  Running the Backup Verification tool ..................................... 213  
  Migrating the MSS hardware .................................................. 213  
  Restoring data on the MSS .................................................... 213  

Migrating each MAS ................................................................. 217  
  Starting the MAS migration .................................................... 217  
  Preparing the new server ....................................................... 220
## Contents

<table>
<thead>
<tr>
<th>Content</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing and administering anti-virus software</td>
<td>220</td>
</tr>
<tr>
<td>Updating Microsoft Windows</td>
<td>220</td>
</tr>
<tr>
<td>Reapply the remote access settings for each MAS</td>
<td>221</td>
</tr>
<tr>
<td>Updating settings in the VMSC</td>
<td>222</td>
</tr>
<tr>
<td>Creating the offline message share, if needed</td>
<td>225</td>
</tr>
<tr>
<td>Restarting messaging services</td>
<td>228</td>
</tr>
<tr>
<td>Completing VMSC setup</td>
<td>230</td>
</tr>
<tr>
<td>Continuing the MAS migration</td>
<td>231</td>
</tr>
<tr>
<td>Completing MSS administration</td>
<td>231</td>
</tr>
<tr>
<td>Verify the MAS host information</td>
<td>232</td>
</tr>
<tr>
<td>Placing the MSS in the Windows domain—MAS#1 only</td>
<td>233</td>
</tr>
<tr>
<td>Restoring data on each MAS</td>
<td>234</td>
</tr>
<tr>
<td>Stopping all MM services</td>
<td>235</td>
</tr>
<tr>
<td>Restoring backed-up MAS data</td>
<td>236</td>
</tr>
<tr>
<td>Restoring Caller Applications—MAS#1 only</td>
<td>238</td>
</tr>
<tr>
<td>Restarting Modular Messaging services</td>
<td>239</td>
</tr>
<tr>
<td>Installing software updates</td>
<td>240</td>
</tr>
<tr>
<td>Performing acceptance tests for a migration</td>
<td>241</td>
</tr>
<tr>
<td>Completing the system migration</td>
<td>242</td>
</tr>
<tr>
<td>Running a DCT analyze on the migrated system</td>
<td>242</td>
</tr>
<tr>
<td>Backing up the system</td>
<td>242</td>
</tr>
<tr>
<td>Running backups on each MAS</td>
<td>242</td>
</tr>
<tr>
<td>Removing old backup files from the MSS</td>
<td>244</td>
</tr>
<tr>
<td>Backing up the MSS</td>
<td>245</td>
</tr>
<tr>
<td>Completing the Modular Messaging system migration</td>
<td>247</td>
</tr>
<tr>
<td>Updating or installing client software</td>
<td>248</td>
</tr>
<tr>
<td>Reducing servers by replacing S3400 servers with S8730 servers</td>
<td>249</td>
</tr>
<tr>
<td>Changing switch integration</td>
<td>251</td>
</tr>
<tr>
<td>Moving to the corporate Windows domain after migration</td>
<td>252</td>
</tr>
<tr>
<td>Appendix A: Installation and upgrade checklists</td>
<td>253</td>
</tr>
<tr>
<td>Modular Messaging on Avaya MAS installation checklist</td>
<td>254</td>
</tr>
<tr>
<td>Modular Messaging on a customer-provided MAS installation checklist</td>
<td>260</td>
</tr>
<tr>
<td>Modular Messaging Release 5.0 upgrade and migration checklists</td>
<td>265</td>
</tr>
<tr>
<td>Modular Messaging Release 3.x or 4.0 on S3500-family server upgrade checklist</td>
<td>266</td>
</tr>
<tr>
<td>Modular Messaging Release 5.0 system migration checklist</td>
<td>269</td>
</tr>
<tr>
<td>Moving the MM system to the corporate Windows domain checklist</td>
<td>274</td>
</tr>
<tr>
<td>Appendix B: Configuring and testing port boards</td>
<td>275</td>
</tr>
<tr>
<td>Overview</td>
<td>275</td>
</tr>
<tr>
<td>Contents</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>When to configure port boards</td>
<td>276</td>
</tr>
<tr>
<td>Supported port boards</td>
<td>277</td>
</tr>
<tr>
<td>Configuring port boards</td>
<td>277</td>
</tr>
<tr>
<td>Configuring T1-QSIG or E1-QSIG boards</td>
<td>279</td>
</tr>
<tr>
<td>Configuring set emulation boards</td>
<td>280</td>
</tr>
<tr>
<td>Configuring analog port boards</td>
<td>282</td>
</tr>
<tr>
<td>Testing the port boards</td>
<td>287</td>
</tr>
<tr>
<td>Preparing for the test</td>
<td>287</td>
</tr>
<tr>
<td>Testing the ports</td>
<td>288</td>
</tr>
<tr>
<td>Appendix C: Installing Dialogic port boards in a customer-provided MAS</td>
<td>291</td>
</tr>
<tr>
<td>Supported MAS port boards</td>
<td>293</td>
</tr>
<tr>
<td>Installing MAS port boards</td>
<td>295</td>
</tr>
<tr>
<td>Preparing for the installation</td>
<td>295</td>
</tr>
<tr>
<td>Setting jumpers and switches</td>
<td>296</td>
</tr>
<tr>
<td>D/480JCT-1T1 and D/600JCT-1E1 or D/600JCT-2E1 QSIG board settings</td>
<td>297</td>
</tr>
<tr>
<td>D/480JCT-1T1-EW and D/600JCT-1-120-EW QSIG board settings</td>
<td>297</td>
</tr>
<tr>
<td>D/82JCT-U PCI Univ set emulation board settings</td>
<td>298</td>
</tr>
<tr>
<td>D/82JCT-U EW set emulation board settings</td>
<td>299</td>
</tr>
<tr>
<td>D/120JCT-LS 12-port analog board settings</td>
<td>300</td>
</tr>
<tr>
<td>D/120JCT-LS-EW port analog board settings</td>
<td>300</td>
</tr>
<tr>
<td>D/41JCT-LS 4-port analog board settings</td>
<td>301</td>
</tr>
<tr>
<td>D/41JCT-LS-EW analog board settings</td>
<td>303</td>
</tr>
<tr>
<td>Installing the port boards</td>
<td>305</td>
</tr>
<tr>
<td>Disabling the Dialogic hardware</td>
<td>306</td>
</tr>
<tr>
<td>Connecting MAS port boards to the switch</td>
<td>307</td>
</tr>
<tr>
<td>Completing the hardware installation</td>
<td>308</td>
</tr>
<tr>
<td>Configuring port boards</td>
<td>308</td>
</tr>
<tr>
<td>Configuring T1-QSIG or E1-QSIG boards</td>
<td>310</td>
</tr>
<tr>
<td>Configuring set emulation boards</td>
<td>311</td>
</tr>
<tr>
<td>Configuring analog port boards</td>
<td>312</td>
</tr>
<tr>
<td>Testing the port boards</td>
<td>313</td>
</tr>
<tr>
<td>Appendix D: Creating a new tone file</td>
<td>315</td>
</tr>
<tr>
<td>Learning tones automatically</td>
<td>316</td>
</tr>
<tr>
<td>Running the PBXpert wizard</td>
<td>316</td>
</tr>
<tr>
<td>Consolidating and saving the TSF file</td>
<td>318</td>
</tr>
<tr>
<td>Using the new TSF in Dialogic Configuration Manager</td>
<td>319</td>
</tr>
<tr>
<td>Learning tones manually</td>
<td>319</td>
</tr>
<tr>
<td>Running PBXpert</td>
<td>319</td>
</tr>
</tbody>
</table>
Adding a new tone set ................................................. 320
Learning tone definitions ........................................... 321
Testing the tone set .................................................. 321
Consolidating and saving the TSF file ............................. 322
Using the new TSF in Dialogic Configuration Manager ......... 322

Appendix E: Updating Modular Messaging software ............. 323
Getting software updates from the Web .......................... 324
Installing software updates on each MAS ......................... 325
Copying files to the MAS ............................................ 325
Installing the updates on each MAS ............................... 326
Installing software updates on the MSS .......................... 328

Appendix F: Moving Modular Messaging services ............... 329
Disabling Modular Messaging services you plan to move ....... 330
Moving Modular Messaging services among servers .............. 331
Moving Call Me, MWI, and Mailbox Monitor ..................... 332
Moving MM Fax Sender service ..................................... 334
Moving Audit server ................................................. 336
Moving Tracing service ............................................. 336
Enabling the services on the correct server ....................... 338
Stopping all Modular Messaging services ......................... 338
Enabling the appropriate services ................................ 338
Restarting messaging services ..................................... 339

Appendix G: Adding an MAS or a Supplementary server to an existing system . . . 341
MAS configuration prerequisites ..................................... 342
Adding a new server to a system in service ....................... 343
Installing the new MAS or a Supplementary server ............. 344
Preparing the MSS for the new servers .......................... 345
Adding a new trusted server on the MSS ......................... 345
Using the DCT to analyze the current configuration ............. 346
Configuring the new server ......................................... 349
Running the configuration wizard .................................. 349
Completing new server configuration ............................. 351
Completing the Add New MAS or Supplementary server ....... 352

Appendix H: Reloading MAS and MSS software ................... 353
Loading new MAS software ......................................... 353
Switching the monitor to show the correct server ................ 353
Loading the new software ......................................... 354
About this book

This book, *Avaya Modular Messaging for Avaya MSS Release 5.0 Installation and Upgrades*, provides instructions for the installation and upgrade of the Avaya Modular Messaging software in an Avaya Message Storage Server (MSS) configuration.

In Release 5.0, new installations of the MSS reside on the Avaya-provided S8730 server hardware that runs on Linux Operating System (OS). All new installations of Messaging Application Server (MAS) software can either reside on Avaya-provided S8730 server hardware that runs on Microsoft Windows 2003 R2 Operating System or customer-provided equipment (CPE) server. Both MAS and MSS on S3500 server hardware can be upgraded to Release 5.0.

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

**Note:**
Avaya does not support S3400-family server hardware in Release 5.0. However, this book provides instructions to migrate to S8730-family server.

Information in this book includes:

- Instructions to install the software for Modular Messaging system that includes initial administration, and acceptance testing
- Instructions to upgrade the software from a Modular Messaging Release 3.x or Release 4.0 system to Release 5.0
- Instructions to migrate Modular Messaging system Release 2.0, Release 3.x or Release 4.0 from an S3400 or an S3500 server to an S8730 server.

**Note:**
Use this document to install an Avaya Modular Messaging system. After the software installation, customers must modify the Modular Messaging system parameters for use at their site. For more information, see the administration topics of the user documentation. For instructions to download the documents, see [Downloading user documentation](#) on page 12.

---

**Intended audience**

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

- Installation and configuration of hardware and software for the Avaya S8730 servers and for the customer-provided (CPE) MAS.
- Upgrade from Release 3.x or Release 4.0 that runs on the S3500 server to Modular Messaging Release 5.0.
About this book

- Migration from Release 2.0, Release 3.x or Release 4.0 to Modular Messaging Release 5.0 that runs on S8730-family server.

Avaya assumes that the users of this book have completed a relevant hardware installation training course. For more information about training, see Related resources on page 5.

Changes to this book

This book includes the following enhancements:

- New software installation procedures
- New upgrade procedures
- New migration procedures

  For information on procedures for staged upgrade of Avaya Modular Messaging Release 2.0, 3.x or 4.0 to Release 5.0 on S8730, see Avaya Message Storage Server Staged Upgrade from Release 2.0, 3.x, 4.0 to Release 5.0 guide.

- Customer-provided equipment (CPE) server as MAS

- Support for S8730 hardware. For hardware specific information, this document refers to Installing the Avaya S8730 Server guide.

Note:

This document only provides the information on software installation, upgrades and migration of the Avaya Modular Messaging system in an Avaya Message Storage Server (MSS) configuration. See Installing the Avaya S8730 Server guide for information on procedures to install and maintain the new hardware.
How to use this book

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

Installing a new system

To install a Modular Messaging system:

1. A project planner must create an Avaya Modular Messaging Data Collection Tool (DCT) data file before the installation is started. Send the DCT data file to the technical support representative at the customer’s site.

2. Print the checklist for a new installation from Modular Messaging on Avaya MAS installation checklist on page 254. Use it to track your progress.

3. Read Chapter 1: Preinstallation requirements on page 7. This chapter describes installation requirements and site preparation, including where to find required documentation, software, and tools that are required to install the Modular Messaging system.

4. Read and use each chapter in the order presented. Follow the procedures in the same sequence as given in the book.

Upgrading a system

To upgrade a Modular Messaging system that already runs on an S3500 server:

1. Obtain the following before you start the upgrade:
   a. The original DCT file for the system or planning forms for the system that runs on Release 3.x.
   b. The latest analyzed DCT file for the system.

2. Print the upgrade checklist from Modular Messaging Release 3.x or 4.0 on S3500-family server upgrade checklist on page 266 to use as a guide.

3. Follow the instructions in Upgrading to Modular Messaging Release 5.0 on S3500-family server on page 145 to upgrade each server.
Migrating a system

To migrate a Modular Messaging system from Release 2.0, Release 3.x or Release 4.0:

1. Obtain the following before you start the migration:
   a. The original DCT file for the system or planning forms for the system that runs on Release 2.0 or Release 3.x.
   b. The latest analyzed DCT file for the system

2. Print the migration checklist from Modular Messaging Release 5.0 system migration checklist on page 269 to use as a guide.

3. Follow the instructions in Migrating to Modular Messaging Release 5.0 on S8730-family server on page 201 to migrate each server.

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

Always use the appropriate user documentation to obtain specific information to plan, to install, to administer, or to maintain an Avaya Modular Messaging system. To view or download the user documentation, see Downloading user documentation on page 12.

Technical assistance

The following technical assistance is available if needed.

Remote support center

Your project manager or systems consultant provides you the telephone number of the appropriate remote support center.

Use the following numbers for technical assistance with Avaya products and services:

- Within the United States and Canada: call 1-800-242-2121
- 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) from the application or the wizard for which you need help.
- MSS: On the Web-interface pages, click the Help button.

Note:

To close the help window, click Close situated at the bottom of the page. If you use the browser button to close the help window, you might leave a hidden help window open. You must close all open Help windows before you can close the browser.
About this book

Training

For information about product training, go to the Avaya Web site at http://www.avaya.com and click Training.

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 Avaya MSS Release 5.0 Installation and Upgrades, Issue 1.0, February 2009.
Chapter 1: Preinstallation requirements

This chapter describes the prerequisites for installing an Avaya Modular Messaging system that uses Avaya S8730-family servers.

Topics in this chapter include:

- Software shipped with the system on page 8
- Obtaining the DCT data file on page 9
- Downloading required software and documentation on page 9
- Security considerations on page 13
- Test equipment recommendations on page 14
- Initial switch and LAN administration on page 15
- Private Windows domain consideration with MM Fax Sender service on page 16
- Corporate Windows domain requirements on page 16

For information on specifications, site requirements, switch and LAN demarcation points for Avaya-provided server, see Installing the Avaya S8730 Server for Modular Messaging.
# Software shipped with the system

Avaya ships the following software with each Modular Messaging system:

<table>
<thead>
<tr>
<th>Media</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Avaya Modular Messaging R5.0 MAS Application—2 DVDs | Use this software to:  
  - Install the Modular Messaging software and optional application programs running on Avaya-provided servers and CPE servers  
  - Upgrade to R5.0 on S3500-family servers |
| Avaya Modular Messaging R5.0—MSS Application disk and MSS OS disk—2 DVDs | Use this software to upgrade to Release 5.0 or to reload the software. |
| **For S8730:** Avaya MODULAR MESSAGING R5.0 MAS for Avaya Store Model S8730 Boot disk | Use this software to reinstall the boot-image software to recover from a hard-disk failure. |
| **For S3500:** Avaya MODULAR MESSAGING R5.0 MAS for Avaya Store Model S3500 Boot disk | |
Obtaining the DCT data file

A DCT data file is used to configure the MSS and each 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 project manager, customer representative, or any responsible person creates this file. The DCT data file has an extension `mmdct`, such as `sitefile.mmdct`.

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 that you carry with you to the customer site.

⚠️ **CAUTION:**

The USB drive must be formatted only as a FAT16 or a FAT32 file system and not as an NTFS file system.

**Note:**

For more information about the DCT, obtain the *Avaya Modular Messaging Data Collection Tool Online Help*; see Downloading user documentation on page 12.

---

**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 this information only from the Avaya Support Web site. Download the information before you visit the customer site. Some of the sites, where Modular Messaging system is installed might not have access to Internet.

⚠️ **Important:**

Always check the Avaya Support Web site at [http://www.avaya.com/support](http://www.avaya.com/support) for any latest updates and information before you install or upgrade. Note 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 10
- [Downloading configuration notes](#) on page 11
- [Downloading the installation and upgrade checklists](#) on page 11
- [Downloading user documentation](#) on page 12

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
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) and software patches for the system:

2. Click the link to FIND DOCUMENTATION and TECHNICAL INFORMATION by PRODUCT NAME.
4. On the Modular Messaging page, select Release 5.0 from the drop-down list.
5. Click Downloads.
6. Download any files needed for the Release 5.0 system. Ensure that you download any instructions required to install the Service Pack or software update.
7. In addition to any other files, download the following:
   - Avaya Modular Messaging 5.0 Outlook Client
   - Avaya Modular Messaging 5.0 DCT Tool. You will use this file to update the DCT data file.
   - (Release 2.0, Release 3.x or Release 4.0 upgrade to R 5.0) Avaya Modular Messaging 5.0 MSS Pre-upgrade and Backup Verification Tool
   - The latest Modular Messaging service pack.
   - The latest Modular Messaging Patch.
8. Copy the downloaded files to a storage device.
9. Bring the storage device with you to the installation site.
Downloading configuration notes

Obtain the configuration notes required to integrate the MAS with the PBX or telephony switch at this site. To obtain the recent copy, complete the following:

2. Click the link to FIND DOCUMENTATION and TECHNICAL INFORMATION by PRODUCT NAME.
4. On the Modular Messaging page, select Release 5.0 from the drop-down list.
5. Click Configuration Notes.
6. Download or print the configuration notes for the switch integration.

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

Downloading the installation and upgrade checklists

Access the PDF version of the checklists for installation and upgrade from the Avaya Support Web site. You can also find the checklists in Appendix A: Installation and upgrade checklists on page 253. To download the checklists:

2. Click the link to FIND DOCUMENTATION and TECHNICAL INFORMATION by PRODUCT NAME.
4. On the Modular Messaging page, select Release 5.0 from the drop-down list.
5. On the Modular Messaging page, click Installation, Migrations, Upgrades and Configurations.
6. Click the following link: Modular Messaging with an Avaya MSS Release 5.0 Installation and Upgrade Checklists.
7. Click Download.
8. From the File Download dialog box, open or save the checklists file.
Preinstallation requirements

Downloading user documentation

User documentation needed for installing a new system is on the Avaya Support Web site:

2. Click the link to FIND DOCUMENTATION and TECHNICAL INFORMATION by PRODUCT NAME.
4. In the release field, click 5.0.
5. On the Modular Messaging page, click Documentation Library (CD Collections).
6. Click Avaya Modular Messaging Release 5.0 Documentation.
7. Click View HTM.
8. Click Avaya Modular Messaging with the Avaya MAS and MSS.
9. To find the user documentation you must do one the following:
   ● continue to click the document links on the left side of the page
   ● click the Search link on the right side of the page and enter the title of a document, such as Administering trusted servers on the MSS.
10. After you find the relevant documentation, either click the document link to view or print the files, or right-click to download the files.
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 protection

To protect password security:

● Do not leave written passwords lying out or allow anyone to see the passwords.

● At the first opportunity, give the passwords directly to the designated customer representative.

● If you suspect that the security of the system was compromised, notify the project manager or the system administrator.

System security protection during installation

To protect system security during the installation:

● Remove all test subscribers and test mailboxes from the system when the procedures instruct you.

● Do not configure any unassigned mailboxes. Unassigned mailboxes are mailboxes that have an extension, but no subscriber assignment.

● Always log off or lock the server if you leave it unattended, even for a short period.
Ongoing system security considerations

Customers must obtain and install the anti-virus software on any Microsoft Windows computer that is to run Avaya Modular Messaging software. Customers must also routinely install updates for Microsoft Windows systems to protect the system from known security weaknesses. Updates include operating system updates and security patches. For more information, obtain "Modular Messaging and security;" see Downloading user documentation on page 12.

Note:
Avaya technical support representatives must follow the specified internal procedures to verify the installed software. If required, the technician 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 have a data display for testing the PBX integration and the Find Me and Call Me features.
  - If the system uses the lamp as the message waiting indicator (MWI), the test telephone must have a lamp. If the system uses a stutter tone as MWI, the telephone must provide the stutter notification.
  - Arrange the test telephones so that 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 required for the installation. 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 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.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Private Windows domain consideration with MM Fax Sender service

When you configure the MM Fax Sender server, an account with the credentials to create a trust relationship between the private and corporate Windows domains must be available or a person from customer’s corporate IT group who has details for an account with the credentials is available. If the IT representative cannot provide the account information during installation, skip the MM Fax Sender configuration and complete the rest of the Modular Messaging installation. Return to Configuring the MM Fax Sender server on page 68 and complete the configuration of the one-way trust when the account information is available.

Corporate Windows domain requirements

Note:
If the MM system will use the private Windows domain, you can skip these requirements.

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

- Creating user accounts in the corporate Windows domain on page 17.
- Creating computer accounts in the corporate Windows domain on page 18.
- Adding RAS and IAS permissions to the technical support account on page 19
Creating user accounts in the corporate Windows domain

⚠️ Important:
Perform this procedure only if you plan to join the Modular Messaging system to the corporate Windows domain.

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

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

2. Click Start > Programs > Administrative Tools > Active Directory Users and Computers. The system opens the Active Directory Users and Computers window.

3. Expand the directory for the corporate Windows domain.

4. Right-click Users and from the pop-up menu, select New > User.

5. In the New Object window, type the user account name, such as techacct or custacct, in both the Full Name and the User logon name fields.

6. Click Next.

7. Type the user account password in both the Password and Confirm Password fields.

8. Select the Password never expires check box.

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

9. Click Next.

10. Click Finish.

11. Repeat this process as needed to make sure you create both technical support and the customer administration support accounts.
Creating computer accounts in the corporate Windows domain

⚠️ Important:
Perform this procedure only if you plan to join the Modular Messaging system to the corporate Windows domain.

The corporate Windows domain administrator creates computer accounts in the corporate Windows domain for all servers in the VMD. This includes the MSS, all MASs, and, if present, the Supplementary server and optional servers, such as the Modular Messaging Web Client:

1. The corporate Windows domain administrator logs into the Active Directory server using a log in that has privileges to add a computer account to the corporate Windows domain.
2. Click Start > Programs > Administrative Tools > Active Directory Users and Computers. The system opens Active Directory Users and Computers dialog box.
3. Expand the directory for the corporate Windows domain.
4. Right-click Computers and from the pop-up menu, select New > Computer.
5. In the New Object window, in the Computer name field, type the server name you want to create, such as mymss or mymas1.
6. Click Change. This specifies that a different user or group can add this computer to the corporate Windows domain.
7. In the Select User or Group window, enter the customer administration account, such as custacct, that you created previously; see Creating user accounts in the corporate Windows domain on page 17.
8. Click Check Names.
9. Click OK.
10. Click Next.
11. Make sure that This is a managed computer check box is NOT selected.
12. Click Next.
13. Click Finish.
14. Repeat this process for each MAS and Supplementary server (if present) in the VMD.
Adding RAS and IAS permissions to the technical support account

You must add RAS and IAS permissions to the technical support account:

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

2. Click Start > Programs > Administrative Tools > Active Directory Users and Computers. The system opens the Active Directory Users and Computers window.

3. Expand the directory for the corporate Windows domain.

4. Click Users.

5. In the right pane of the window, double-click RAS and IAS Servers to open the Properties window.

6. In the RAS and IAS Servers Properties window, click the Members tab.

7. Click Add. The system opens the Add window.

8. Make sure that Select These Object Types includes Computers in the list. If not, click Object Types and select the Computers check box, then click OK.

9. In the Object Name field, type the server name, such as MYMAS1, and click Check Names.

10. Verify that the correct computer name is shown underlined in the list box.

11. Repeat the last two steps to add all Modular Messaging servers to this list.

12. Click OK to close this window.

13. Click OK to close the RAS and IAS Servers Properties window.

14. In the right pane, double-click the technical support account.

15. In the Properties window for the remote access account, click the Dial-in tab.

16. Under Remote Access Permission (Dial-in or VPN), select Allow access.

17. Leave CallBack Options set at No Callback.

18. Click OK on each open window until they are closed.
Chapter 2: Performing initial MSS administration

This chapter describes how to perform initial administration on the Message Storage Server (MSS).

Note:
Ensure that you have completed the tasks described in Installing the Avaya S8730 Server for Modular Messaging guide.

Installing a Modular Messaging system involves many steps, therefore, use the system installation checklist in Appendix A: Installation and upgrade checklists on page 253. Check off the step as you complete it, to track your progress.

Topics in this chapter include:

- Logging on to the MSS on page 22
- Starting the MSS configuration using a DCT data file on page 24
- Configuring the MSS manually on page 26
- Setting the time and date on page 31. You can configure the MSS automatically or manually, however, you must set the time and date manually.
Performing initial MSS administration

---

Logging on to the MSS

After you turn on the hardware, log on to the Message Storage Server (MSS). As you have not yet administered the system, you can access the MSS only from the console that is connected to the KVM switch.

To log on to the MSS from the console:

1. If the Message Storage Server (MSS) is not turned on, press the power button to turn on the server now.

2. Verify that the monitor shows the MSS.
   - For a 2-port KVM switch, the MSS is connected to one of the computer ports.
   - For an 8-port Belkin KVM switch, the MSS usually is connected to the first computer port on the switch. The port is labeled VGA 01.

3. If the monitor displays a different server, toggle the port to show the MSS.
   - To have a 2-port Belkin KVM switch show a different server:
     a. Press Scroll Lock twice.
        The LED on top of the Belkin KVM switch starts to blink.
     b. Type the port number. For example, type 1 for port 1.
   - To have an 8-port Belkin KVM switch show a different server:
     a. Press Scroll Lock twice within 2 seconds.
     b. Select the server that you want to be displayed on the monitor using 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 using the keyboard. For example, type 1 for port 1.

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

4. When the boot is complete, you see the message Press Enter to return to prompt.... Press Enter.

5. At the localhost login: prompt, log on to the MSS as craft.
   The server displays the Messaging Administration web interface.

Note:
If the system displays any certificate warnings, click OK.
Adjusting the display settings, if needed

Check the display quality of the monitor screen.

- If the display is poor, correct the display quality using the steps in this section.
- If the monitor displays system information well enough for an initial administration, continue with Setting the time and date on page 31.

To adjust the monitor display settings:

1. Click Log Off.
   - If the display is so poor that you cannot see the mouse pointer, exit by press Ctrl+Alt+Backspace to exit.
2. Log on to the console as monitor. Use the password of monitor.
3. In the Display Settings window:
   a. Click Settings to adjust the resolution of the screen or the depth of the color.
   b. Click Hardware to change the type of the monitor or the video board.
      1. To change the type of the monitor or the video board, click Configure.
      2. Select the required hardware type, and click OK.
4. Click OK to close the Display Settings window.
5. If the system prompts you to confirm, click OK.
6. At the localhost login prompt, log on to the system as craft. Check if the display quality has improved.
7. If the display quality is still poor, return to Step 2 and change the settings.
8. If the changed settings does not improve the display, the customer must use a different monitor.
Starting the MSS configuration using a DCT data file

This section explains how to start the automatic configuration of the MSS using a DCT data file. Do not use a DCT data file prepared from a system analysis or from an earlier release of the system. For more information, see Obtaining the DCT data file on page 9.

The MSS configuration happens in two phases. This procedure explains phase one. You must then configure each MAS and Supplementary server (if present), as explained in Configuring the Avaya MAS on page 41 for Avaya MAS or Configuring a customer-provided MAS on page 85 for a CPE MAS and proceed with phase two of the MSS configuration as outlined in Completing initial MSS administration on page 101.

Use the following steps to configure the MSS using a DCT data file:

1. Log on to the MSS as craft. See Logging on to the MSS on page 22.
2. Insert the storage device that contains the DCT data file into the MSS.
3. If you want to change the time, manually set the time and date of your system, even if you plan to use an NTP server. See Setting the time and date on page 31. You cannot set up the NTP server now.
4. From the Server Administration menu on the Messaging Administration web interface, click Configure Using DCT. The system opens Configure MSS using DCT page.
   
   **Note:** If the DCT file is configured for INADS alarming, ensure that the modem is connected or the configuration fails.

5. Select the DCT data file from the storage device and click Fresh Configuration.
6. On the page that displays the configuration information from the DCT data file, click ONE of the following:
   
   - If the configuration information is correct, click Continue Configuration to continue with the next step.
   - If the configuration information is incorrect, you must change the information in DCT file using the following steps:
     a. Click Cancel Configuration
     b. Return to the Windows computer and change the information
     c. Save the data file on the storage device. For information about changing the DCT data file see Avaya Modular Messaging Data Collection Tool Online Help.
     d. If you are able to correct the DCT data file, repeat tasks from step 1, using the updated DCT data file. However, if you cannot make the corrections, contact technical support.
7. On the pop-up screen that appears, click OK to continue with the configuration.
   
   The page displays the status of the configuration, automatically refreshing the information until this part of the configuration is complete.
8. If this part of the MSS configuration is successful, the page displays ‘Finish MAS installation before continuing MSS configuration.’ message at the bottom of the page. Do one of the following:

- If you are installing a Supplementary server with this Modular Messaging system, modify the Supplementary server trusted server entry that was create by the MSS automatic configuration tool:
  
a. Under the Messaging Administration of the Messaging Administration web interface, click Trusted Servers. The system displays Manage Trusted Servers page.
  
b. Highlight the Trusted Server with a service name of Supplementary Server. Click Edit the Selected Trusted Server.

The server displays the Edit Trusted Server page.

- In the Special Type field, click Messaging Application Server from the drop-down list.
  
d. Click Save.

- Start MAS configuration using the procedures outlined in Configuring the Avaya MAS for an Avaya-provided MAS or Configuring a customer-provided MAS for a customer-provided MAS. You may now set up an NTP server, if one is available as instructed in Setting the time and date on page 31.

  Note:
  
  Do not click Continue Configuration at this time. You must proceed with phase two of the MSS installation as described in Completing initial MSS administration on page 101 only after you complete MAS configuration.

- If you see FAILURE on the status display, contact Avaya technical support. When you make the corrections, return to Step 4, except that the button on the Configure MSS using DCT page now displays Continue Configuration.
Configuring the MSS manually

You do not need to configure the MSS manually. You can use the DCT data file to configure the MSS. Use the following procedures if you choose not to use the DCT data file or if you choose to change any configuration while the installation is underway.

Use the following procedures to manually configure the MSS:

- **Setting up network addressing** on page 27
- **Setting the time and date** on page 31
- **Setting up the MSS local machine** on page 32
- **Setting up the trusted servers** on page 33
- **Rebooting the MSS** on page 39
Setting up network addressing

You must configure the MSS to work on both the corporate LAN and the private LAN.

⚠️ CAUTION:
Do not use the examples shown in this book!

To set up the MSS to work on the corporate and private LANs:

1. Log on to the MSS as craft; see Logging on to the MSS on page 22.
2. From the Server Administration menu on the Messaging Administration web interface, click TCP/IP Network Configuration.
3. Complete the following information on the Configure Network Addressing page (for more information about each field, click the Help button or the field name):
   a. For Host Name, enter the MSS NetBIOS machine name, such as mymss.
   b. For Default Gateway Address, enter the corporate default gateway IP address for the MSS.
4. To administer Corporate LAN settings (you will verify Private LAN settings later in this section):
   a. For Primary Name + Domain, enter the full corporate computer name for the MSS, such as mymss.loc.avaya.com.
   
   Note:
   The Primary Name + Domain name is a combination of the Host Name and the Domain Name fields on this page. However, the Primary Name might be different from the host name, depending on the corporate setup. For example, primname.loc.avaya.com.
   b. For IP Address, enter the corporate IP address for the MSS.
   c. If the system prompts you that changing the IP address will cause a momentary loss of service, click OK.

⚠️ Important:
Remember when you verify the corporate subnet mask, the private IP address and the corporate IP address must not use the same subnet. If same subnet is in use, change the private subnet mask; see step c on page 28. For example in the following table, ensure that the IP address part (in bold) of both the corporate and private network are different.
Performing initial MSS administration

d. For **Subnet Mask**, type the corporate subnet mask for the MSS.

e. **Optional:** For **Aliases**, type any required aliases for this interface. All aliases must be unique and cannot duplicate any other computer names or aliases, either on the Modular Messaging system or on the corporate network. To enter multiple aliases, separate the names with a space.

If you leave the field blank, the system automatically provides an alias for the corporate full computer name of the MSS. The alias is the corporate NetBIOS name for the MSS, which is the primary name for the MSS full computer name up to the first period. For example, the system provides the alias `mymss` for the full computer name `mymss.loc.avaya.com`.

f. For **Network Media Type**, use the default `auto detect` option unless you have a problem connecting to the network switch. Some routers do not automatically detect the correct settings. For more information about media types, click **Help**.

5. Verify the Private LAN settings and update only if necessary:

   a. For **Primary Name + Domain**, the system displays the predefined private system name for the MSS, `mss1`.

   b. For **IP Address**, use the correct MSS private IP address from the range of IP addresses that the private network uses at this site.

   **CAUTION:**
   
   You must use the same private IP address range for the MSS that you use for each MAS. Ensure that the private network settings in the Modular Messaging Data Collection Tool (DCT) match the settings on this page. For more information, see [Configuring MASs using an existing DCT data file](#) on page 44.

   The private IP address of the MSS must use the subnet that you have chosen for the private LAN. If the system prompts you that changing the IP address will cause a momentary loss of service, click **OK**.

---

Table 2: Example for valid private and corporate IP addresses

<table>
<thead>
<tr>
<th>Example</th>
<th>Corporate IP address</th>
<th>Corporate subnet mask</th>
<th>Private IP address</th>
<th>Private subnet mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>135.9.83.107</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Invalid</td>
<td>192.168.1.100</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
Configuring the MSS manually

⚠️ Important:
Remember when you verify the private subnet mask, the private IP address and the corporate IP addresses must not use the same subnet. If the same subnet is in use, change the private subnet mask. See Example for valid private and corporate IP addresses on page 28.

c. For Subnet Mask, verify the private subnet mask for the MSS.

d. Leave Aliases for the private network blank.

e. For Network Media Type, verify if you have selected the correct type. The type is usually auto detect. For more information about media types, click Help.

6. Administer the DNS (Domain Name Service) server as appropriate:

- If you do not use a corporate DNS, set the Enable DNS field to No. Continue with Step 7.
- To use a corporate DNS, set Enable DNS to Yes. Continue with the following steps:
  a. For Domain Name, type the corporate domain name.
  b. For Name Server, add any IP addresses listed for corporate DNS servers that the MSS uses. Press Enter after each IP address.

Note:
The MSS accepts only IP addresses in this field, even if the system uses Dynamic Host Configuration Protocol (DHCP) to assign most IP addresses.

c. You must specify a Search Order only if the system must search across multiple domains. If a Search Order is required:
   1. Always enter the name of the corporate domain shown in the Domain Name field first. Press Enter.
   2. Add any other domain names listed for the MSS Search order of DNS domains. Press Enter after each domain name.

7. Click Save.
Performing initial MSS administration

8. After the system displays the Network Addressing status, click **Log Off** (which appears in the menu at the top left of the page).

   **Note:**
   
   If you do not log off, the system times out and logs off automatically.
   
   Ensure that no Help windows are open in the background, or they prevent the browser from closing. To close a Help window, click the close link at the bottom of the Help page.
   
   The system displays the prompt:
   
   `hostname login:`
   
   **Note:**
   
   Avaya recommends you to wait for at least 1 minute before you log into the system again.

9. Verify that `hostname` in the login prompt is the same as that you entered in Step 3-a under Setting up network addressing on page 27. If the hostname is not the same:

   a. Log on and return to the Network Addressing page using the **craft** account. See Steps 2 and 3 under Setting up network addressing on page 27.
   
   b. Type the host name correctly. Verify all your network configuration settings.
   
   c. Click **Save**.
   
   d. Log off from the MSS.
Setting the time and date

⚠️ Important:

Set the time and date the first time you log on to a new MSS and BEFORE you configure any MAS.

This topic explains how to set the time and date on the MSS:

1. Log on to the MSS as craft; see Logging on to the MSS on page 22.
2. From the Server Administration menu, click Date/Time/NTP Server.
   The server displays the Administer Linux Date and Time page.
3. If the time zone is incorrect, from the Time Zone drop-down menu select the correct time zone (changing Time Zone requires a reboot).
4. Do one of the following to manually set the time or connect to an NTP server:
   - For manual entry, click Manual:
     a. For Date, select the month and day. Type the current year, for example 2008.
     b. For AM/PM, select the type of time you use: AM, PM, or 24-hour clock.
     c. For Time, select the hours and minutes.
   - To connect to an NTP server, click NTP Time Server:
     a. Enter the name of the NTP server or the IP address.
     b. Click Add NTP Server.
       The server will automatically update and maintain your system's time and date.
5. If you made any changes to the page, click Save.
6. If you see a security warning about unencrypted information, click Continue.
7. If the system prompts you to run the time.bat file to synchronize the time with all MASs, click OK.
   The Date and Time page displays the new settings.
8. Click Log Off.
9. If the system again prompts you to run the time.bat file on all MASs, click OK.
10. Log on to the MSS as craft once again, see Logging on to the MSS on page 22.
11. If you are manually configuring the MSS, continue with Setting up the MSS local machine on page 32.
Setting up the MSS local machine

To set up a profile for the local machine for MSS:

1. If not already logged in, log on to the MSS as **craft**; see *Logging on to the MSS* on page 22.
2. From the Messaging Administration menu on the Messaging Administration web interface, click **Networked Machines**. The system opens Manage Networked Machines page.
3. Highlight the MSS that you are administering.
4. Click **Edit the Selected Networked Machine**.
5. On the **Edit Networked Machine** page, complete only the following fields:
   a. For **Machine Name**, verify the customer-specified MSS host name. If no corporate LAN is available, the Machine Name remains as LocalHost (with an IP of 127.0.0.1).
   b. For **Mailbox Number Length**, select a number from the list.
   c. For **Password**, type the password to use for LDAP directory updates. This password enables networking with other messaging servers, such as other MSS or Message Networking servers. Type the same password in the **Confirm Password** field.
   d. Under **Mailbox Number Ranges**, you might require the **Prefix** field.
   e. In the field **Starting Mailbox Number** field, type the appropriate starting mailbox extension number for the address range. For example, for a five-digit dial plan, you might type **55000**.
   f. In the **Ending Mailbox Number** field, type the appropriate ending mailbox extension number for the address range. For example, for a five-digit dial plan, you might type **55999**. To enter multiple address ranges, repeat Steps e and f.

   **Note:**
   
   If you are enabling MultiSite feature, you do not have to set the start and end mailbox number. Ignore step 5e and step 5f.

6. Scroll down, and click **Save**.
7. At the confirmation message, click **OK**.
Setting up the trusted servers

You must add a trusted server for each MAS and Supplementary server, if present, that is to run Avaya Messaging Application Server (MAS) software. You must also set up all other required servers that are in this voice mail domain.

**Note:**
You can have a maximum of six MASs that includes a Supplementary server (if present) in the system. However, only five of the MASs can handle calls. The sixth MAS can be an Avaya-provided or customer-provided Supplementary server. The Supplementary server can provide all other services except handling calls. This section describes how to set up MASs and the Supplementary server, if present, as trusted servers.

See the following tasks for setting up trusted servers:
- Adding each MAS as a trusted server on page 33
- Adding the MWI trusted server, if used on page 35
- Adding optional trusted servers on page 36
- Updating the IMAP4 password and the system protocols on page 37

Adding each MAS as a trusted server

To set up each MAS or Supplementary server in the system as a trusted server:

1. Log on to the MSS as **craft**; see Logging on to the MSS on page 22.
2. On the Messaging Administration web interface, under **Messaging Administration**, click **Trusted Servers**.
   The system opens the Manage Trusted Servers page.
3. Click **Add a New Trusted Server**.
   The system opens the Add Trusted Server page.
4. Complete the following fields:
   a. In the **Trusted Server Name** field, type the customer-specified NetBIOS name for this MAS, such as **mymas1**.
   b. In the **Password** field, type the LDAP password used for all MASs in this Modular Messaging system. Type the password again in the **Confirm Password** field.
Performing initial MSS administration

c. In the **Machine Name / IP Address** field, enter the correct private IP address for this MAS. To find the correct private IP address for this MAS, see Table 3: **Private IP addresses for each MAS by IP address range** on page 34. Use the IP address that matches the MAS you are currently entering and the IP address range that is used for this site. To determine the correct IP address range for this site.

⚠ **CAUTION:**
You must use the same private IP address range on the MSS that you will use on each MAS. Ensure that the private network settings in the Modular Messaging Data Collection Tool match the settings on this page. For more information, see **Configuring MASs using an existing DCT data file** on page 44.

<table>
<thead>
<tr>
<th>Private network IP address range</th>
<th>MAS#1 IP address</th>
<th>MAS#2 IP address</th>
<th>MAS#3 IP address</th>
<th>MAS#4 IP address</th>
<th>MAS#5 IP address</th>
<th>MAS#6 IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1 to 10.255.255.254</td>
<td>10.255.1.250</td>
<td>10.255.1.249</td>
<td>10.255.1.248</td>
<td>10.255.1.247</td>
<td>10.255.1.246</td>
<td>10.255.1.245</td>
</tr>
<tr>
<td>172.16.0.1 to 172.31.255.254</td>
<td>172.31.1.250</td>
<td>172.31.1.249</td>
<td>172.31.1.248</td>
<td>172.31.1.247</td>
<td>172.31.1.246</td>
<td>172.31.1.245</td>
</tr>
</tbody>
</table>

d. In the **Special Type** field, click **Messaging Application Server**, when you add a trusted server for an MAS or a Supplementary server.

The **Special Type** selection populates the other fields with the required values.

5. After you verify or update the information, click **Save**.

6. At the confirmation message, click **OK**.

7. To add a subsequent MAS or a Supplementary server, if any, repeat Steps 3 through 6 for each MAS in the system.
Adding the MWI trusted server, if used

If the Message Waiting Indicator (MWI) Server is to be installed on any MAS, add a trusted server for it now.

To add a Message Waiting Indicator (MWI) trusted server:

1. On the Messaging Administration menu of the Messaging Administration web interface, click **Trusted Servers**. The system displays **Manage Trusted Servers** page.
2. Click **Add a New Trusted Server**.
   The server displays the **Add Trusted Server** page.
3. Complete the following fields on the **Add Trusted Server** page:
   a. For **Password** and **Confirm Password**, type a password that identifies the MWI server to all messaging servers in this Modular Messaging system.
   b. For **Machine Name / IP Address**, type the private IP address of the MAS or Supplementary server on which you want to install the MWI Server feature

   **CAUTION:**
   You must use the same private IP address range on the MSS that you use on the MAS. Ensure that the private network settings in the Data Collection Tool match with the settings on this page. For more information, see Configuring MASs using an existing DCT data file on page 44.
   c. For **Special Type**, select **MWI Server** from the drop-down list.
      The **Special Type** selection populates the other fields with the required values. Do not change the value **VVSTS** in the **Server Name** field.
4. Click **Save**.
5. At the confirmation message, click **OK**.
6. Continue as appropriate:
   - If you have to install a Supplementary server at this site, continue with Adding each MAS as a trusted server on page 33.
   - If you have added all trusted servers for this site, continue with Updating the IMAP4 password and the system protocols on page 37.
Adding optional trusted servers

You use the **Add Trusted Server** page to add other trusted servers to the messaging network. Servers might include a Mailbox Manager server, a Provision server, or a Site Administration (ASA) server. Often, the customer administrator adds these servers after initial installation.

If directed, you can add one or more optional trusted servers as follows:

1. On the Messaging Administration menu of the Messaging Administration web interface, click **Trusted Servers**. The system displays **Manage Trusted Servers** page.

2. Click **Add a New Trusted Server**.

   The server displays the **Add Trusted Server** page.

3. Complete the following fields on the **Add Trusted Server** page:

   a. In **Trusted Server Name** field, type the customer-specified NetBIOS name for this server, such as *mymas6*.

   b. In **Password** field, type the LDAP password to be used for all MASs in this Modular Messaging system. Type the password again in the **Confirm Password** field.

   c. In **Machine Name / IP Address** field, continue as appropriate:

      - For a corporate setup that uses DHCP addressing, type the full corporate computer name using all lowercase letters. For example, type *provision.loc.avaya.com*.

      - For a corporate setup that uses static IP addresses, type the corporate IP address for this server.

      - For Supplementary server, type the private network IP address for this server as. To enter the correct private IP address for this server, see Table 3: Private IP addresses for each MAS by IP address range on page 34.

   d. Enter any other information required for this type of server and connection.

   e. In the **Special Type** field, click **Messaging Application Server** to add a trusted server for an MAS or for a Supplementary server.

      The **Special Type** selection populates the other fields with the required values.

   **Note:**

   For more information, use the help or obtain "Administrering trusted servers on the MSS;" see Downloading user documentation on page 12.

4. Click **Save**. At the confirmation message, click **OK**.
Updating the IMAP4 password and the system protocols

On all systems, you must update the password for the IMAP trusted server as follows:

1. From the Messaging Administration web interface, click **System Administration**.
   
   The server displays the Administer System Attributes and Ports page.

2. Under **SYSTEM ATTRIBUTES**, enter the password for Internet Message Access Protocol (IMAP) in this messaging network:
   
   a. Type the **IMAP4 TUI Password**.
   
   b. Type the same password in the **Confirm IMAP4 TUI Password** field.

3. Scroll down to the **SYSTEM TCP/IP PORTS** section. Enable any required protocols and access permissions for desktop clients, web applications, or other required services at this site. For a list of protocols required for various applications, see [Table 4: TCP ports to enable for Modular Messaging client applications](#).

   For example, to enable Microsoft Outlook client access:

   a. Next to **LDAP Port** 389, select **Enabled**.
   
   b. Next to **IMAP4 Port** 143 and **SMTP Port** 25, select **Enabled**.
Performing initial MSS administration

Table 4: TCP ports to enable for Modular Messaging client applications

<table>
<thead>
<tr>
<th>Client</th>
<th>LDAP Port 389</th>
<th>LDAP Dir Update Port 56389</th>
<th>IMAP4 Port 143</th>
<th>IMAP4 SSL Port 993</th>
<th>POP3 Port 110</th>
<th>POP3 SSL Port 995</th>
<th>SMTP Port 25</th>
<th>SMTP SSL Port 465</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Lotus Notes client</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Microsoft Outlook client</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Modular Messaging Web client</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard IMAP client</td>
<td>Optional</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>Optional</td>
</tr>
<tr>
<td>Standard IMAP client with SSL</td>
<td>Optional</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>Optional</td>
</tr>
<tr>
<td>Standard POP3 client</td>
<td>Optional</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Standard POP3 client with SSL</td>
<td>Optional</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>Optional</td>
</tr>
<tr>
<td>UCC server for Speech Access</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Networked Modular Messaging or Message Networking</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Multi-site or Site Administration</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mailbox Manager</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provision</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
To provide desktop client access, you must also set the options for MAS Privacy as appropriate and **Restrict Client Access** for the appropriate class of service. For more information, see [Administering classes of service](#) on page 110.

4. Click **Save**.
Rebooting the MSS

To reboot the MSS, complete the following:

1. From the Utilities menu, click **Reboot Server**.
   The server displays the Reboot Server page.

2. Click **Reboot**.

3. At the reboot warning message, click **OK** to continue.
   The system displays status messages as the server shuts down the messaging software.
   The software shutdown can take several minutes.

   **Note:**
   You do *not* have to wait for the reboot process to complete to continue with the installation.
Performing initial MSS administration
Chapter 3: Configuring the Avaya MAS

This chapter applies only to an Avaya-provided Messaging Application Server (Avaya MAS) and Supplementary server installation. This chapter describes how to configure an Avaya Messaging Application Server (MAS) and a Supplementary server, if any. You must configure each Avaya Messaging Application Server (MAS) and Supplementary server in the VMD beginning with the first MAS. The servers must work both on the corporate local area network (LAN) and on the private LAN used for the Modular Messaging system.

If you are using customer-provided MAS, use the procedures described in Configuring a customer-provided MAS on page 85 to configure the CPE MAS.

Topics in this chapter include:

- Displaying an MAS from the console on page 42
- Completing MAS configuration prerequisites on page 43
- Configuring MASs using an existing DCT data file on page 44
- Preparing the new server on page 47
- Configuring MAS port boards on page 52
- Configuring the voice mail system on page 53
- Continuing the installation on page 83

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Displaying an MAS from the console

Because the system is not yet administered, you can access a server from the console (monitor) that is connected to another server through the KVM switch.

1. To turn on the S8730-family server, press the power button on the front of the server, until the LED turns green. For more information, see Installing the Avaya S8730 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. Select the server to display using 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.
Completing MAS configuration prerequisites

Ensure that you complete these requirements before you begin the MAS configuration:

● Obtain the required software and documentation; see Downloading required software and documentation on page 9.

● Obtain the current DCT (MMDCT.exe) from the Avaya support web site (do NOT use the DCT on the applications DVD); see Downloading software updates on page 10.

● For systems that join the corporate Windows domain, create the user and the computer accounts in the corporate Windows domain; see Creating user accounts in the corporate Windows domain on page 17 and Creating computer accounts in the corporate Windows domain on page 18.

● Install the required system hardware; see Installing the Avaya S8730 Server for Modular Messaging guide.

● Complete the initial MSS administration; see Chapter 2: Performing initial MSS administration on page 21.

● Continue to use the "New Modular Messaging installation" checklist in Appendix A: Installation and upgrade checklists on page 253.
Configuring MASs using an existing DCT data file

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

⚠️ CAUTION:

Configure each Avaya Messaging Application Server (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 43.

2. Ensure that the MSS 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 42.

   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.


6. On the Locate Configuration Data screen, select the appropriate DCT data file for the site. If the required DCT data file is not populated, 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.

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.
Configuring MASs using an existing DCT data file

c. For an Avaya-provided server, select **MSS 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.
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.

10. On the Messaging Application Server Number screen, verify that the **MAS number** field shows the correct number 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 reboots. After the reboot, 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 a new S8730-family server, the product key sticker located on the right-hand edge of the server chassis. Record the Windows product key.
   c. Click **Next**.
   The Avaya Modular Messaging Configuration Wizard displays the configuration status on the Configuring System screen. The server reboots several times. However, you do not need to log on manually. The entire process takes about 30 minutes.

**Note:**
If the system displays a Configuration Credential LDAP failure, verify that the MSS is running. The MSS must be available during the MAS configuration process. If the MSS is running, do the following:
   - Verify that LDAP password in the DCT data file match with that of MSS. See **Setting up the MSS local machine** on page 32.
   - Verify that you have properly connected the private network LAN cable.

When the server configuration is complete, the progress bar stretches across the screen and the **Next** button becomes active.

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

13. Click **Next**.

14. On the Avaya Modular Messaging Wizard Completed screen, click **Finish**.

15. Complete all tasks outlined in **Preparing the new server** on page 47 applicable for the server before you run the Avaya Modular Messaging Configuration Wizard on the subsequent MAS.
Preparing the new server

This section describes how to update and protect the new server. See the following:

- **Updating Windows Internet Explorer 7 security** on page 47
- **Installing and administering anti-virus software** on page 48
- **Updating Microsoft Windows** on page 49
- **Entering RAS IP addresses on each MAS** on page 50

## Updating Windows Internet Explorer 7 security

**Note:**

Use this procedure if you have to install any third-party software from a mapped network drive. If you install the third-party software from a disk or other removable media, such as a USB storage device, you can skip this procedure and continue with **Installing and administering anti-virus software** on page 48.

Before you install any third-party software, such as anti-virus software, from a mapped network drive, you need to update Windows Internet Explorer 7 security. If you do not make this update and use a domain account, such as `custacct`, to install third-party software, Windows will not allow you to install.

1. If you have not already updated, map the network drive which contains the third-party software.
2. Launch the Windows Internet Explorer 7 browser.
3. A window appears that states Windows Internet Explorer Enhanced Security is enabled; click **OK**.
4. From the browser, select **Tools > Internet Options**.
5. From the Internet Options window, select the **Security** tab.
6. In the "Select a zone to view or change security settings" box, click **Local intranet**.
7. Click **Sites**.
8. On the Local intranet window, in the "Add this web site to the zone" field, type the universal naming convention (UNC) path of your mapped network drive, using the `\computername\share` format, and click **Add**.
9. Click **OK** to close the Local intranet window.
10. Click **OK** to close the Internet Options window.
Installing and administering anti-virus software

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

1. You might need to install the anti-virus software using the local administrator account. If you cannot install the required files using the customer account login, log off and then log in using the local administration account name.

2. Install the anti-virus software using the installation method that is appropriate for this site.

3. Configure the anti-virus software to work correctly with Avaya Modular Messaging software.

**CAUTION:**

Some anti-virus software such as McAfee VirusScan Enterprise 8.0i blocks the port 25 by default. The Modular Messaging system uses TCP/IP port 25 to send messages from the MAS to the MSS. To enable port 25, open the anti-virus program. Change the access protection properties to unblock port 25.

Guidelines for using anti-virus software on an Avaya Modular Messaging server include:

- Avoid using a message-scanning method that can greatly impact the performance of the Avaya servers. Avaya recommends to use "on-demand" scanning, where scans run at scheduled intervals. Do not use "on access" scanning that runs when the system access a file. This reduces the performance of the server. Some anti-virus software applications, by default, sets to on-access scanning at system startup. To disable this feature, you must change the on-access scan properties.

- Avaya recommends you administer the anti-virus software as follows:
  - Scan the hard disk at least once in a week during off peak hours. Avaya recommends a daily scan. You can run scans on multiple Modular Messaging servers simultaneously. However, do not schedule the anti-virus scan when the system saves the backup data on the MAS. By default, the MAS backups start between 9:00 PM and 11:00 PM every night, depending on the number of MASs in the system.
  - Schedule virus definition updates to occur automatically at least once per week. Have the updates occur before the next scheduled scan time to ensure that the scan uses the latest data (DAT) files. However, do not schedule updates to occur during a virus scan. For example, you might implement a virus definition update at 8:45 PM, and schedule the anti-virus scan for midnight, after the MAS backup completes.
  - If the anti-virus software identifies a virus, the program takes a backup of the detected files before they are cleaned or deleted by the scanner. You can configure to automatically delete the infected files after a specified number of days and manage the files.

For more information about anti-virus software, obtain "Modular Messaging and security;" see [Downloading user documentation](#) on page 12.
Updating Microsoft Windows

A new Avaya MAS contains the most current Microsoft Windows software at the time it is shipped. After installation, you must install the latest updates for Microsoft Windows, including operating system updates and security patches. These software updates protect the system from known security weaknesses. Check with the appropriate Windows administrator for the software update procedures to use at this site.

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.
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 required by the technical support organization.

⚠️ CAUTION:
If Avaya is to support this system, you must enter the RAS IP addresses that the Avaya Automatic Registration Tool (ART) provides. Otherwise, remote access for Avaya technical support will not work. For more information, see Registering the system in ART on page 130.

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, such as MYMAS1.
4. Verify authentication:
   b. On the right-pane, double-click Connections to Microsoft routing and remote access.
   c. Click the Edit Profile... button.
   d. On the window that appears, select the Authentication tab.
   e. Make sure that all checkboxes (except for the Unauthenticated access) are selected. If necessary, clear the Unauthenticated access checkbox.
   f. Click OK.
   g. If a dialog box appears, click No.
   h. Click OK again.
5. Right-click the server name, such as MYMAS1 and from the pop-up menu, select Properties.
6. Set up authentication methods:
   a. In the local Properties window for the server, click the Security tab.
   b. Click Authentication Methods...
   c. On the window that appears, select both Microsoft encrypted authentication version 2 (MS-CHAP v2) and Microsoft encrypted authentication (MS-CHAP).
   d. Make sure all other checkboxes are blank. If necessary, deselect the checkboxes.
   e. Click OK.
7. Set up a static IP address pool as follows:
   a. In the local Properties window for the server, 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. For example, the range might show all zeroes or start with 192.168.2.
      ! CAUTION: If Avaya will support this server, do not use the preprogrammed IP addresses, such as 192.168.2.200. You must Edit or 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.
8. Close the Configure window.
Important:
If this MAS does not contain Dialogic port boards, skip the rest of this section and continue with Configuring the voice mail system on page 53.

The Avaya Modular Messaging Configuration Wizard automatically configures the dialogic port boards for the following switch integrations.

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

If this MAS does not use one of the automatic-configuration switch integrations, you must configure the Dialogic port boards manually.

1. Continue with Appendix B: Configuring and testing port boards on page 275.
2. After you configure and test the Dialogic port boards, continue with Configuring the voice mail system on page 53.
Voice mail system configuration falls into three areas:

- Domain-wide administration that must be done once for each new installation. You usually configure these settings on MAS#1.
- Domain-wide features, such as Call Me or Message Waiting Indicator (MWI) that can be enabled on any MAS.
- Configuration information specific to an MAS, such as Modem Dialout alarming or port board administration.

This section describes how to configure the key parameters to make the new system operational. Complete the tasks in this section to obtain 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 Downloading user documentation on page 12 in Avaya Modular Messaging MAS Administration Guide.

Note:

The system prompts you to restart the MAS Voice Server service several times during this procedure. However, you must restart the service only as directed in this guide. Restart the service before you enter the modem extension numbers as instructed in Configuring MAS-specific parameters on page 74. Restart the service again when you complete the configuration.

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 11.

Topics in this section include:

- Configuring required domain-wide features on page 54
- Verifying license installation and specifying TTS sessions on page 62
- Adding the Supplementary server name into the security configuration on page 62
- Entering Product ID for current MAS on page 63
- Configuring specific features as needed on page 64
- Configuring MAS-specific parameters on page 74
- Restarting the messaging services on page 77
- Verifying basic operation of the MAS on page 80
- Continuing the installation on page 83
Configuring required domain-wide features

Note:
Do the following tasks only for MAS#1. For additional MASs, go to Configuring specific features as needed on page 64.

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

- Specifying languages on page 55
- Verifying that Modular Messaging service has started on MAS#1 on page 55
- Configuring TUI and audio settings on MAS#1 on page 56
- Configuring the PBX type on MAS#1 on page 57
- Configuring serviceability settings on MAS#1 on page 58
- Obtaining and installing a license on MAS#1 on page 60

For a new installation, do these tasks on MAS#1.

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.

Specify the preferred Modular Messaging 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.

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. Double-click the Monitor icon on the desktop.
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, and if the status is Started, close Monitor and proceed with the steps in Configuring TUI and audio settings on MAS#1 on page 56.
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:
   a. Repeat steps 3 and 4.
   b. Right-click MM Service Connector and select Start
10. Proceed with the next task.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Configuring TUI and audio settings on MAS#1

You must configure the settings in this section once for each Modular Messaging system. For a new installation, do these procedures on MAS#1.

To configure settings that are required for all Modular Messaging setups:

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

   The Voice Mail System Configuration window opens. You can see a list of MASs that are present in the messaging system.

   **Note:**
   Perform 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, such as vmdom, double-click Telephone User Interface.
   
   a. On the General tab, set Number of Digits in a Mailbox to match the length of Mailbox numbers required for this system. If MultiSite is enabled, the Number of Digits in a Mailbox field is unavailable.

   b. Click OK to close this window.

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

3. 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 States 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. For better sound quality, set the audio encoding to G.711 μ-Law for SIP integration. G.711 encoding is required to support TTY/TDD devices.

   b. Click OK to close this window.

   c. If you changed the audio encoding, a "restart" box appears. Click OK, but you do not have to restart now.
Configuring the PBX type on MAS#1

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 11. 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. The Avaya Modular Messaging Configuration Wizard automatically configures many settings for some 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 3.
   - If no PBX type is listed, continue with step 2.
2. If there are no PBXs available for the Modular Messaging system, 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 Dialogic Set Emulation.
   b. In the PBXs list box, select the type of switch integration that you have, such as Avaya G3 Set Emulation.
   c. Click OK to close the window.
   d. In the Voice Mail System Configuration window, expand PBXs.
   e. If PBXs are already available, expand the PBXs item under the voice mail domain, such as vmdom.
3. Double-click the PBX entry under PBXs.
4. Use the configuration notes to set up or verify the specific PBX parameters required for the type of switch integration you use. Obtain the configuration notes as instructed in Downloading configuration notes on page 11.
Configuring serviceability settings on MAS#1

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

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

To set up serviceability settings for the system:

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 Alarm Origination type of alarming to be used for the Modular Messaging system: Inactive, SNMP, Modem Dialout, or Internet.

   Note:
   The MAS must have a modem connected if you select Modem Dialout alarming. You must also set up the correct type of alarming on the MSS. For more information, see Setting up alarming on the MSS on page 133.

3. Unless directed otherwise, you must 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, you may need to set your community. To set the community, click the Communities tab, select Add and complete the following:
   - For Community, click the field and enter a community name. This name is used as validation in communications between the SNMP client and the SNMP server.
   - For Apply To, from the drop-down menu, select either Traps or Both (do not select Queries).

5. If you selected SNMP alarming, click the SNMP Trap Destinations tab.

   Note:
   During an upgrade, enter the SNMP trap destination and community details that you recorded from the Release 3.x or Release 4.0 system.
6. To set, click **Add** and complete the following:

- For **IP Address/Host**, enter the IP address or host name for the trap destination.
- For **Community**, select a community name from the drop-down menu. This name is used as security validation in communications between the SNMP client and the SNMP server. The drop-down menu list is populated from the Communities tab.
- For **Type**:
  - Select **INADS** to send alarms back to Avaya through older Service Selection Gateway (SSG) devices.
  - Select **OAM** (Operations, Administration, and Maintenance) for use with customer NMSs.
- For **Port**, usually accept the default value (162); otherwise, specify a port.

7. If you selected Internet alarming, click the **Internet Proxies** tab. To set, click **Add**:

- For **Avaya/Business Partner Primary Destination**, enter the Avaya proxy primary IP address or fully qualified domain name (FQDN).
- For **Avaya/Business Partner Secondary Destination** enter the Avaya proxy secondary IP address or FQDN.
- For **Enable Customer Proxy Servers**, if the enterprise network configuration does not pass HTTP, then set Internal alarming to use proxy servers by clicking this selection to enable. The following fields become active:
  - For **Customer Primary Proxy Server**, enter the customer proxy primary IP address or FQDN.
  - For **Customer Secondary Proxy Server**, enter the customer proxy secondary IP address or FQDN.

8. Click **OK** to close the Serviceability - Voice Mail Domain window.
Obtaining and installing a license on MAS#1

You must obtain a license and install it for each Modular Messaging system. Do this procedure on MAS#1.

**Note:**
You must use Remote Feature Activation (RFA) to obtain a license for all new and upgraded systems. For the latest information, go to [http://rfa.avaya.com](http://rfa.avaya.com) Web site. For complete licensing steps and contact information for RFA assistance, see *Getting Started with RFA for Modular Messaging* on the RFA Web site.

If the Modular Messaging system is being implemented with an Avaya Communication Manager server, and if a T1-QSIG, E1-QSIG, or IP H.323 switch integration is used, the person who requests the Modular Messaging RFA license must also request the QSIG Supplementary Services package. The QSIG Supplementary Services package is an entitlement captured within the Communication Manager RFA license. It must be set to **ON** and uploaded to the Communication Manager server, in addition to the Modular Messaging RFA License. Contact your Avaya representative for more information.

To obtain and install a license for the Modular Messaging system, complete the following steps:

1. A registered RFA user must generate a license request for the new system using RFA. The request must include all the required information described in *Getting Started with RFA for Modular Messaging*. The procedure varies with location. However, the on-site installer must provide the voice mail domain identifier (VMD ID) to complete the license request.

2. Obtain the unique VMD ID that identifies this Modular Messaging system to complete a license request. To obtain the VMD ID:
   a. In the **Voice Mail System Configuration** window, right-click **Licensing** and select **Copy Host ID to clipboard**.
   b. Open a text-editor application such as Notepad to record this information.
   c. Right-click and select **Paste** to copy the VMD ID from the clipboard to the document.
   d. Save the file. For example, save the file into **My Documents** as *mymas1-vmdid.txt*.
   e. Send the file that contains the VMD ID to a location that can access the Internet or e-mail location. Use any method that is required, such as FTP, memory stick, and so on. Send the file to the RFA-authorized party, or use the file yourself to complete the RFA license request through the RFA Web site. Procedures vary according to location.
3. The authorized person completes the license request using RFA. The person then downloads or sends the license file by e-mail to the appropriate location.

4. If another party must complete the license request, you can continue with the installation until you receive a valid license file. At that time, return to Installing the license on page 61.

⚠️ CAUTION:

For most switch integrations, you can continue with the installation through acceptance testing using a default license that supports up to ten subscribers.

For IP SIP integrations, however, you must receive and install a valid license before you can complete acceptance testing (you can, however, add subscribers before installing the license).

Installing the license

After you obtain the license file, install the license as follows:

1. Copy the license file, such as wlmNNNNNNlicense.xml, to the MAS using the method preferred by the customer, such as FTP, memory stick, and so on. Avaya recommends to copy the license file on MAS#1 in the C:\Avaya_Support directory.

2. To install the license, in the Voice Mail System Configuration window, right-click Licensing and select Import License.

3. On the License Import Wizard welcome screen, click Next.

4. On the Importing the license screen, click Browse.

5. Navigate to the location where the license file is stored, such as C:\Avaya_Support.

6. Double-click the appropriate *.xml license file. If more than one file is present, verify that you select the correct one.

7. Click Next to install the license.

8. When the procedure is complete, click Finish.

⚠️ CAUTION:

If an error message states that the license is not valid, you must obtain a new license file. The event log on the MAS on which the license import failed might contain additional information about the reason for failure. Verify that the license request contains the correct VMD ID for this system. Return to Step 2 and submit a new license request through RFA.

9. Continue with Verifying license installation and specifying TTS sessions on page 62.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Verifying license installation and specifying TTS sessions

After you install the license file, verify the license values and set up the TTS sessions on the MAS you are configuring:

1. In the Voice Mail System Configuration window, double-click **Licensing**.
2. In the Licensing - Voice Mail Domain window, on the **General** tab, verify that the system displays the correct values as per the license agreement.
3. Click the **Text-to-Speech** tab.
   a. For the current MAS, double-click the TTS engine to set up, such as **Text to speech, ScanSoft RealSpeak, Any Language**.
   b. In the **Edit Sessions** window, enter 12 sessions for the MAS if it handles calls.
   c. Click **OK**.
   d. Repeat this step for each licensed TTS engine.
4. Click **OK** to close the Licensing - Voice Mail Domain window.

**Note:**

After you complete the licensing procedure, you must restart service for the changes to take effect. For this procedure, see **Restarting the messaging services** on page 77.

Adding the Supplementary server name into the security configuration

*Use this procedure only when you configure the Supplementary server.*

When you install Supplementary server into an existing VMD, you must add the Supplementary server name to the Security Admin access control list (ACL) in the VMSC. If you do not add the server to the Security Admin ACL, the services installed on the Supplementary server fail to run.

Use the following steps to add the Supplementary server to the access control list in VMSC:

1. Click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**. The system opens the **Voice Mail System Configuration** window.
2. Double-click **Security Roles**.
3. Click **Servers**.
4. Click **Add**.
5. Click **Object Types** and select the **Computers** check box.
6. In the **Enter object** field, enter the Supplementary server machine name (that is, *name$*).
7. Click **Check Names**.

8. Click **OK**.

After you complete the configuration of the new Supplementary server, move the required Modular Messaging services to the server. Use the procedures described in *Moving Modular Messaging services* on page 329.

---

### 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. For more information, see *Registering the system in ART* on page 130.

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 the Avaya MAS

Configuring specific features as needed

During installation, MMCW enables services and TTS languages specified in the DCT. 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 or on a remote computer running the VMSC application.

Note:
Some of the important notes to be considered while configuring these features:

- In a multiple-MAS system, configure specific features only after you complete basic configuration of all MASs in the system. Some features, such as MWI, TTS, and offline access to messages, require all MASs in the VMD to be working.

- 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 were 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 331.

- 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 Release 5.0 with the Avaya MSS MAS Administration Guide**.

To configure specific features on an MAS:

1. Use the Voice Mail System Configuration (VMSC) program.
   
   If this window is not already open, click **Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration**.

2. Configure the features that are required for this MAS:

   - **Configuring Call Me service** on page 65
   - **Configuring Notify Me** on page 65
   - **Configuring MWI service** on page 66
   - **Configuring MM Audit Service** on page 67
   - **Configuring the MM Fax Sender server** on page 68
   - **Configuring languages and multi-lingual TTS** on page 71
   - **Configuring offline access to messages** on page 73
Configuring Call Me service

To configure the Call Me service for the VMD:

1. In the Voice Mail System Configuration window, under the VMD, such as vmdom, double-click Call Me.
2. In the Call Me - Voice Mail Domain window, on the General tab, click the Enable Call Me checkbox.
3. For MAS Call Me Server, specify the name of the server on which the Call Me service will be enabled, such as MYMAS2. If this field is blank:
   a. Click ... next to the field.
   b. In the Select Computer window, enter the name of the MAS you chose as your MAS Call Me server.
   c. Click Check Names.
   d. Click OK to accept the MAS name and close the window.
4. Click OK to close this window.

Note:
Because Call Me service and Message Waiting Indicator (MWI) service use the Mailbox Monitor Server, you must enable both services on the same server.

Configuring Notify Me

The Notify Me feature is configured by default. To configure the Notify Me for the VMD:

1. In the Voice Mail System Configuration window, under the VMD, double-click Notify Me.
2. On the General tab, select the Enable Notify Me checkbox.
3. Click OK.
Configuring the Avaya MAS

Configuring MWI service

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

1. In the **Voice Mail System Configuration** window, under the VMD, such as `vmdom`, double-click **Message Waiting Indicator**.

2. In the Message Waiting Indicator - Voice Mail Domain window, on the **General** tab, select the **Enable Message Waiting Indicator (MWI)** checkbox.

3. For **MAS MWI server**, specify the name of the server on which to enable the MWI service, such as `MYMAS2`. If this field is blank:
   a. Click ... next to the field.
   b. In the Select Computer window, enter the name of the MAS you chose as your MAS MWI server.
   c. Click **Check Names**.
   d. Click **OK** to accept the MAS name and close the window.

4. For the **Limit requests** and **Maximum requests per minute** fields, use the values specified in the configuration notes for your PBX integration type.

5. In the **Messaging Application Servers that support MWI** box, list all MASs that have a port group set up to support MWI. To add a server name:
   a. Click the **Add** button at the top of the list box. The **Add** button looks like a dashed box.
   b. The list box displays a data entry field and a ... button. Click the ... button.
   c. In the Select Computer window, double-click the name of each MAS that has ports allocated to support MWI, such as `MYMAS2`.
   d. Repeat Steps b and c to add any other MASs that support MWI, such as `MYMAS1`.
   e. Click **OK** to close the Select Computer 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 this window.

**Note:**

Because Call Me service and Message Waiting Indicator (MWI) service use the Mailbox Monitor Server, you must enable both services on the same server.
Configuring MM Audit Service

To configure the MM Audit service for the VMD:

1. In the **Voice Mail System Configuration** window, under the VMD, double-click **Auditing**.
2. On the **General** tab, select the **Enable Auditing** checkbox.
3. In the **Audit server** field, enter the name of the server that hosts the MM Audit server, or use the browse button ... to select the name:
   a. In the Select Computer window, enter the name of the MAS you chose as your Audit server.
   b. Click **Check Names**.
   c. Click **OK** to accept the MAS name and close the window.

   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 server, MAS or supplementary, that you select and configure 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 Audit database resides or use the browse button ... to select the server.
6. In the **Database name** field, enter the name of the Audit Server SQL database.
7. In the **Database instance** field, enter the name of the Audit Server SQLDatabase instance containing audit events.
8. Click **OK** to close this window.

Audit service can be configured to use the syslog protocol to allow third-party system administration tools to be used with Modular Messaging. For more information, see the *Avaya Modular Messaging MAS Administration Guide*. 

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Configuring the MM Fax Sender server

*IP H.323 switch integration does not support fax.*

Complete the following steps on the MAS in your VMD that runs the Modular Messaging Fax Sender service.

**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 the MM Fax Sender server:
- Configure the MM Fax Sender server in VMSC
- Configure one-way trust in a private Windows domain
- Share the MM 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 VMD, such as *vmdom*, double-click **Fax**.
2. In the **Fax - Voice Mail Domain window**, on the **General** tab:
   a. Click the **Fax Enable** checkbox.
   b. Next to **MM Fax Sender server**, click **Browse**.
   c. In the Select Computer window, enter the name of the MAS you chose as your MM Fax Sender server.
   d. Click **Check Names**.
   e. Click **OK** to accept the MAS name and close the window.
   f. For **Fax Mailbox**, enter the mailbox number that is used for outgoing faxes on the MSS.

**Note:**
The mailbox number must match the number configured in the **Fax Mailbox Number** field of Configure Subscriber Management page in Messaging Administration > Messaging Attributes of the Messaging Administration web interface. For more information, see Administering special mailboxes on page 112.

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

**Note:**
The Application Event Viewer displays an error stating that the fax mailbox could not be opened. This is because the fax mailbox is not yet created. The fax mailbox is created in phase 2 of MSS administration as described in Completing initial MSS administration on page 101. The fax feature does not work until the MSS administration is complete.

Use the following steps to configure one-way trust between the private Windows domain and the customer's corporate Windows domain.

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

**Important:**
When you configure the MM Fax Sender server, an account with the credentials to create a trust relationship between the private and corporate Windows domains must be available or a person from customer's corporate IT group who has an account with the credentials is available.
If the IT representative cannot provide the account information during installation, skip the MM Fax Sender server configuration and complete the rest of the Modular Messaging installation. Proceed with Configuring the MM Fax Sender server on page 68 and complete the configuration of the one-way trust when the account information is available.

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

To share the MM Fax Printer, perform this procedure on the same MAS that runs the MM Fax Sender service:

1. Verify that Windows Fax Service is **Started** and set to **Automatic**.
2. Click **Start > Settings > Printers and Faxes**.
3. In the **Printers and Faxes** window, right-click the **Fax** and select **Properties**.
4. Click the **Security** tab.
5. Add the Network Service user and assign that user **Print**, **Manage Printers**, and **Manage Documents** permissions.
6. Click the **Sharing** tab.
7. Select the **Share this printer** checkbox. Leave the share name as **Fax**.
8. Select the **List in the directory** check box.
9. Click **Additional Drivers**. The system opens the **Additional Drivers** dialog box.
10. Select the client operating systems installed on the network that can use the Fax Printer. The Fax Printer drivers are downloaded when you first connect the system to the Fax Printer.
11. Click **OK**.
12. Click the **Security** tab.
13. Verify that **Everyone** is assigned Fax permissions on the share.
Configuring the voice mail system

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

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

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

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

7. Exit all windows.

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

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

Configuring languages and multi-lingual TTS

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

1. In the Voice Mail System Configuration window, under the VMD, such as vmdom, double-click Languages.
2. In the Languages - Voice Mail Domain window:
   a. For Primary Language, select the primary announcement language (prompt set) that is to be used at this site.
   b. If multi-lingual Text-to-Speech (TTS) is used at this site:
      1. Click the Enable Multilingual Text to Speech checkbox.
Configuring the Avaya MAS

2. In the list box, select all the languages to be used for TTS at this site.
3. Click OK to close this window.
Configuring offline access to messages

⚠️ CAUTION:

Set up offline access only after all MASs in the system are configured, including the Supplementary server, if present.

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 checkbox.

4. If this system has multiple MASs:
   a. Select the Synchronize offline messages with remote store checkbox.
   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 one of the following formats:
      - In the private Windows domain: \computername.privdom.local\sharename, such as:
        \mymas2.privdom.local\RemoteOfflineStore
      - In the corporate Windows domain: \computername.corpdom.com\sharename, such as:
        \mymas2.corpdom.com\RemoteOfflineStore

5. Change any other parameters in this window as needed. For more information, see Avaya Modular Messaging MAS Administration Guide; see Downloading user documentation on page 12.

6. Click OK to close the window.

7. Restart the MAS service on all MASs in the VMD:
   a. Double-click the Monitor icon on the desktop.
   b. Select Services (Local) in the left pane, if the item is not already selected.
   c. In the right pane, select MM Messaging Application Server from the available services.
   d. Right-click MM Messaging Application Server and select Restart.

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

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 following tasks for each MAS as required:

- Configuring Modem Dialout alarming, if used on page 74
- Configuring port boards and switch integration on page 75

Configuring Modem Dialout alarming, if used

If the MAS uses Modem Dialout alarming, configure the service now. You must administer Modem Dialout alarming individually for each server that uses it. The server requires a modem and the Messaging Application Server service to be enabled for Modem Dialout alarming to work.

To set up Modem Dialout alarming on this MAS:

1. In the Voice Mail System Configuration window, expand Message Application Servers.
2. Expand the entry for the MAS, such as MYMAS1.
3. Double-click Serviceability to set up dial-out information for this MAS.
4. In the Serviceability window on the Modem Dialout tab:
   a. For 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. For more information, see Installing the Avaya S8730 Server for Modular Messaging guide.
   b. For Phone number, enter the complete telephone number that 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. For Modem setup, enter the modem initialization (setup) string if one is required for the modem to make alarm notification calls.
5. Click OK to close this window.
6. When prompted restart service.
Configuring port boards and switch integration

**Note:**

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

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

**Note:**

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

**Automatic configuration**

The Configuration Wizard automatically configures many of 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 use any of these switch types:

1. Use the MM configuration notes to complete and verify the MAS settings.
2. Administer all required settings on the switch and PBX on the MAS.

**Manual configuration**

If you specified **Other** for the switch integration type, you must always configure both the MAS settings and the PBX 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, select **Telephony Configuration Wizard**.
4. Complete all steps in the wizard, as prompted. Use the configuration notes as required.

**Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.**
5. After you complete the configuration wizard, you must restart messaging service to configure the voice ports:
   a. Restore the Monitor window if you minimized it, or double-click the Monitor icon on the desktop.
   b. Click Services (Local) in the left pane, if the item is not already selected.
   c. In the right pane of the Monitor window, select MM Messaging Application Server. Right-click and select Stop. Do not use Restart.
   d. When service is stopped, right-click MM Messaging Application Server again and select Start.

   The system restarts the messaging service.

   **Note:**
   When you restart messaging service, the Monitor window immediately shows the status as Started. However, 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. In the left pane, expand Event Viewer (Local), and then click Application.
      2. Refresh the window display periodically until you see Telephony User Interface event 1241, TUI service has been enabled. You can then proceed.
      3. Ignore error event 1807. This error is normal until you configure the postmaster mailbox.

   f. When service is restarted, minimize the Monitor window.

6. In the Voice Mail System Configuration window, expand Message Application Servers. Some values might already be set. Use the configuration notes for this PBX integration.
   a. Expand the entry for this 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 11.
   c. Double-click PBX Type. Select the same type of PBX service as you did in Configuring the PBX type on MAS#1 on page 57. 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 for this system. Use the configuration notes to specify or confirm the settings that this switch integration requires.
   f. Determine the maximum number of MWI sessions to specify at one time.
Restarting the messaging services

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

1. Restore the Monitor window if you minimized it, or double-click the Monitor icon on the desktop.

2. Click Services (Local) in the left pane, if the item is not already selected.

3. Restart messaging service to enable any changes you made in the VMSC:

   a. In the right pane of the Monitor window, select MM Messaging Application Server.

   b. Right-click and select Stop.

   c. When service is stopped, right-click MM Messaging Application Server again and select Start. The system restarts the messaging service.

   When you restart the messaging service, the Monitor window immediately shows the status as Started. However, the service might actually take several minutes to start. The time it takes depends on the number of port boards installed and the integration method. Track the status as follows:

   d. In the left pane, expand Event Viewer (Local), and then click Application.

   e. Refresh the window display periodically until you see Telephony User Interface event 1241, TUI service has been enabled. You can then proceed.

4. Verify that the Modular Messaging services required for the MAS are started:

   a. In the Monitor window, select Services (Local) in the left pane.

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

      ● Services that are required for this server must show Started and a startup type as Automatic.

      ● Services that are not required on this server must show a blank status and a startup type as Disabled. For more information, see Table 5: Enabling Modular Messaging services in a VMD.
### Table 5: Enabling Modular Messaging services in a VMD

<table>
<thead>
<tr>
<th>Modular Messaging service name</th>
<th>Condition for enabling service</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM Messaging Application Server</td>
<td>Enable on each MAS and the Supplementary server, if present.</td>
</tr>
<tr>
<td>MM Service Connector</td>
<td></td>
</tr>
<tr>
<td>Avaya SPIRIT</td>
<td></td>
</tr>
<tr>
<td>MM Alarming Server</td>
<td></td>
</tr>
<tr>
<td>MM Audit Service</td>
<td></td>
</tr>
<tr>
<td>MM Event Monitor Server</td>
<td></td>
</tr>
<tr>
<td>MM Fault Monitor</td>
<td></td>
</tr>
<tr>
<td>MM Performance Monitor Server</td>
<td></td>
</tr>
<tr>
<td>MM Process Monitor Server</td>
<td></td>
</tr>
<tr>
<td>MM Call Me ¹</td>
<td>Enable on only one server in each VMD, either on an MAS or the Supplementary server, if present.</td>
</tr>
<tr>
<td>MM Fax Sender ²</td>
<td></td>
</tr>
<tr>
<td>MM Mailbox Monitor ²</td>
<td>See the <em>Avaya Modular Messaging Concepts and Planning Guide</em> for the recommended load balancing of services between multiple servers.</td>
</tr>
<tr>
<td>MM MWI ²</td>
<td></td>
</tr>
<tr>
<td>MM Tracing Service</td>
<td></td>
</tr>
</tbody>
</table>

1. The Call Me, MWI, and Mailbox Monitor services must always be enabled on the same server.
2. IP H.323 switch integration does not support MM Fax Sender functionary.

- 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**.  
  4. Refresh the screen to verify that all **MM** services that are *not* required for this server are **Disabled**. Repeat for each service as needed.

⚠️ **CAUTION:**  
All **MM** services that are *not* required for this server must be set to **Disabled** before you perform the next step (4 c). Serious problems occur if you activate a service on multiple servers when it is supposed to run on only one server in the VMD.
c. If the **Status** for any **MM** service that is required for this server is **Stopped** or blank:

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, repeat Step c.

5. When configuration is complete, close all open windows.

6. *For a multiple-MAS system*, after you configure the last MAS, you must restart service on all servers in the VMD. The following properties require a restart of all servers in the voice mail domain:

   - Audio Encoding
   - Fax
   - Languages
   - Licensing
   - Messaging
   - Offline Access
   - PBXs

   **Note:**

   Any feature that you alter in the VMSC that produces a prompt to restart voice service requires a restart of all servers in the VMD. For convenience, you can restart all the MASs in the VMD once at the end of the installation.

   To restart the Modular Messaging services on all MASs in the voice mail domain, switch the console to each MAS and repeat this procedure, **Restarting the messaging services** on page 77.
Verifying basic operation of the MAS

Before continuing, verify the basic functionality of the MAS. Continue with:

- Verifying call-handling capability on page 80
- Verifying alarming setup on page 81
- Verifying Tracing Service operation on page 82
- Verifying Audit service on page 83
- Continuing the installation on page 83

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 119.

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

This test requires the receiving computer, to be set up and ready to receive alarms.

- For a Modem Dialout setup, the USB modem must be connected and configured for the MAS to send or receive alarming information. The MAS must be set up with a valid product ID; see Entering Product ID for current MAS on page 63.

- For information about setting up SNMP alarming, obtain "Administering SNMP on the MSS;" see Downloading user documentation on page 12. Avaya recommends that you do any additional SNMP administration after the Modular Messaging system is set up and running.

Run the following test 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 alarm setup details such as the type of alarm that is set up, the product ID for the MAS. 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 alarm settings, and then run the test again:

   - For all systems, see Configuring serviceability settings on MAS#1 on page 58.

   - For systems that use Modem Dialout, also check Configuring Modem Dialout alarming, if used on page 74.

6. Type exit and press Enter to close this window.

   **Note:**

   For instructions on accessing the MAS alarm or error logs, obtain Avaya Modular Messaging Software Messaging Application Server Administration; see Downloading user documentation on page 12.
Verifying Tracing Service operation

If you have enabled the Tracing Service software on an MAS or Supplementary server, test the Tracing Service operation as follows:

1. Click Start > Programs > Avaya Modular Messaging > Operation 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.
   c. Click the checkbox for Live Mode.
   d. Verify that all the Select Types checkboxes are checked.
   e. Under Selection Activities, verify that the All Activities checkbox is checked.
   f. Click OK.
3. Confirm that the Tracing Service can connect to all MASs in the VMD.
4. Confirm that the Operation History (OPH) viewer displays the collected OPH events.
5. Close the OPH Viewer. If the system prompts you to save the session, click No.

Note:
Without additional configuration, the Operation History Viewer will only function properly on the server with the Tracing Service running. For more information about using the Operation History Viewer, obtain the Avaya Modular Messaging MAS Administration Guide; see Downloading user documentation on page 12.
Verifying Audit service

Use the MM Audit Log Viewer to view the 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 (use this 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. From the dialog box, 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 the *Avaya Modular Messaging MAS Administration Guide*.

---

Continuing the installation

Continue the installation as appropriate:

- If you have additional MASs to configure, repeat the tasks in this chapter for the next MAS. Return to Configuring MASs using an existing DCT data file on page 44.
- If all MASs are now configured, continue with Chapter 5: Completing initial MSS administration on page 101.
Chapter 4: Configuring a customer-provided MAS

This chapter applies only to a customer-provided equipment (CPE) MAS installation. The chapter describes how to set up a Messaging Application Server (MAS) or a Supplementary Server that is provided by the customer to support Avaya Modular Messaging software. The CPE MAS must have two network interface cards (NICs), one to connect to the corporate LAN and the other to connect to the private LAN.

If you are installing an Avaya-provided MAS, do not use the procedures described in this chapter. See Chapter 3: Configuring the Avaya MAS on page 41.

⚠️ 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 equipment (CPE) 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:

- CPE MAS configuration prerequisites on page 86
- Preparing the CPE MAS on page 87
- Configuring the CPE MAS on page 95
- Completing the CPE MAS configuration on page 98

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
CPE MAS configuration prerequisites

Ensure that you complete these requirements before you start the CPE MAS configuration:

- Obtain the required software and documentation; see Downloading required software and documentation on page 9.

- Obtain the current DCT (MMDCT.exe) from the Avaya support web site (do NOT use the DCT on the applications DVD); see Downloading software updates on page 10.

- For systems that join the corporate Windows domain, create the user and the computer accounts in the corporate Windows domain; see Creating user accounts in the corporate Windows domain on page 17 and Creating computer accounts in the corporate Windows domain on page 18.

- Install the required dialogic port boards only on the CPE MAS, which uses switch integration that use Telephony boards. For more information, see Installing Dialogic port boards in a customer-provided MAS on page 291.

- Complete the relevant pre-installation requirements, as described in Preinstallation requirements on page 7.

- Complete the initial MSS administration as described in Chapter 2: Performing initial MSS administration on page 21.

- Continue to use the "New Modular Messaging installation" checklist in Modular Messaging on a customer-provided MAS installation checklist on page 260.
Preparing the CPE MAS

Complete the following procedures to set up each CPE MAS server to support Avaya Modular Messaging services.

- **Installing Microsoft Windows 2003 R2 operating system** on page 87
- **Setting a computer name** on page 87
- **Running recommended disk checks** on page 87
- **Installing and enabling Microsoft Windows services on CPE MAS** on page 88
- **Installing Microsoft Windows updates and security patches** on page 90
- **Installing Microsoft Windows 2003 SP2** on page 90
- **Adjusting system values** on page 90
- **Network connections** on page 92
- **Verifying network adapters and bindings** on page 93
- **Changing the Power Management settings** on page 93

---

**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 CPE MAS** on page 88.

---

**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 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 tools periodically:

- **Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.**
Configuring a customer-provided MAS

- disk Defragmenter system tool
- `chkdsk` command

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

# Installing and enabling Microsoft Windows services on CPE MAS

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

## Installing Microsoft Windows services

Complete the following steps to install the required Windows services:

1. Log on to the CPE MAS using an account that has permissions to install software on this computer, such as the local administrator account.
2. Insert the Microsoft Windows Operating System disk 1 in the CPE MAS drive.
3. Open **Control Panel**, and then double-click **Add or Remove Programs**.
4. On the left pane, click **Add/Remove Windows Components**.
5. Install Microsoft Windows services:
   a. In the **Windows Components Wizard** window, highlight **Application Server**, and click **Details**.
   b. In the **Application Server** window, ensure that you select the following items:
      - Application Server Console
      - ASP.NET
      - Internet information Services (IIS)
      - Message Queuing
   c. In the **Application Server** window, highlight **Internet Information Services (IIS)**, select if the check box is clear.
   d. Click **Details**.
   e. Ensure that you select the following services:
      - NNTP Service
      - SMTP Service
      - World Wide Web Service
   f. Click **OK**.
   g. In the same window, highlight **World Wide Web Server** and click **Details**. Ensure that the **World Wide Web Service** check box is selected.
Preparing the CPE MAS

h. Click OK. The system closes the World Wide Web Service window.

i. Click OK. The system closes the Internet Information Services (IIS) window.

j. Click OK. The system closes the Application Server window.

6. In the Windows Components Wizard window, highlight Management and Monitoring Tools and click Details.

7. In the Windows Components Wizard window, select the Microsoft .NET Framework 2.0 check box.

8. In the Windows Components Wizard window, highlight Networking Services and click Details.
   a. Select Domain Name System (DNS) and click OK. The system closes the Networking Services window.

9. In the Windows Components Wizard window, select the Fax Services check box.

10. Click Next.
    a. Select Do Not Share Fax Printer.
    b. Click OK.

11. Complete the wizard to install the selected services.

12. When the installation is complete, close the Add or Remove Programs window.

Enabling Microsoft Windows services

After you have installed the software, use the following steps to enable each installed service:

1. Right-click My Computer and select Manage.

2. In the Computer Management window, in the left pane, expand Services and Applications, and then click Services.

3. In the right pane, scroll down to the first new service that you installed and double-click the service. The system opens the Properties window.
   a. On the General tab, set the Startup type to Automatic.
   b. Click Apply.
   c. Under Service status, click Start.
   d. Wait for the service to start, and then click OK to close this window.

4. Repeat steps 2 and 3 to enable each service you installed. Note that only a subset of these services might be present on a MAS.

5. When you have enabled the services, close all open windows.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Configuring a customer-provided MAS

Installing Microsoft Windows updates and security patches

After the CPE MAS is installed, 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.

Installing Microsoft Windows 2003 SP2

Verify the service pack version on each CPE MAS and install an update if needed. 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.

Adjusting system values

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

**Note:**
Modular Messaging Release 5.0 configures the server to use a 3GB address space. If you want to revert back to the Windows default value, then contact Avaya support.

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:
   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 values for Windows 2003 R2:
   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. In Processor Scheduling, select Background services.
      2. In 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:
         - In Paging file size for selected drive, set both the Initial size and Maximum size to the default value plus 11 MB.
Configuring a customer-provided MAS

- Click Set.
- Click OK to close this window.

4. Click OK to close the Performance Options window.

  e. On the Advanced tab, under Startup and Recovery, click Settings.

  f. In the Startup and Recovery window, under System failure, verify that the Automatically restart is selected. Click OK.

  g. Click OK. The system closes the System Properties window.

4. Restart the server.

- If you are prompted to restart the server, click Yes.
- If the system does not prompt you, manually restart the server now. Use one of the following steps:
  a. Press Ctrl + Alt + Del, and then click Shut Down.
  b. Select Restart from the drop-down list and click OK.

The server restarts.

Network connections

For a CPE MAS install of Modular Messaging, the Modular Messaging Configuration Wizard assumes that any network connection, called Local Area Connection, is connected to the corporate LAN.

To ensure that the network connections are correctly set up, you must use the Network settings control panel. Use the following steps to set up the network connections:

1. From the Start menu, select All Programs > Accessories > Communications and Network Connections. Or from the control panel, double-click Network Connections or right-click on Network Connection icon in the notification area and select Open Network Connections.

2. Ensure that the Network Connections window is in Details mode.

- On View menu, click Details.

3. Ensure that Name and Status columns are visible.

4. Disconnect all LAN cables from the server.

5. Insert the corporate LAN cable into one of the network adaptors. In the Network Connections window, observe which of the connection changes its state from Unplugged to Connected.

- If the state of Local Area Connection changes to Connected, then the corporate LAN cable is inserted into the correct Network Adaptor for the Corporate LAN. Do not change the position of the network cable.
Preparing the CPE MAS

- If the state of Local Area Connection remains Unplugged, then move the corporate LAN cable to the other Network Adapter.

**Note:**
If you have installed a CPE MAS or a Supplementary server, which runs a non-English version of Windows 2003 R2 operating system, you must rename the display name of corporate local area connection to Local Area Connection and other connection to Local Area Connection 2.

⚠️ **Important:**
The system does not support more than two network cards.

6. Connect the private LAN (Local Area Connection 2) cable to the vacant Network Adapter.

Do not manually configure the IP addresses for the NICs. The Modular Messaging Configuration wizard configures the IP Addresses using the information in the DCT data file.

---

**Verifying network adapters and bindings**

You must complete the following steps to verify the search order in which private and corporate LANs are ordered on an CPE MAS:

2. Right-click and select Properties. The system opens the Network Connections window.
3. From the Advanced menu, click Advanced Settings.
4. In the Adapters and Bindings tab, from the list of connections, ensure that the connection to the private LAN (Local Area Connection) appears above the connection to the corporate LAN (Local Area Connection 2). This is to ensure that MAS accesses private LAN before the corporate LAN.

**Note:**
If the Local Area Connection 2 is not the first entry, select Local Area Connection 2. Use the up arrow key to move the item to the first position. Click OK.

5. Click OK.
6. Close all open Windows.

---

**Changing the Power Management settings**

Use the following steps to change the Power Management settings for the LAN connection:

1. Click Start > Settings > Network Connections.
   The system opens the Network Connections window.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
2. Select the LAN connection, right-click and select **Properties**.
   a. Click **Configure** in the General tab.
   b. Click the **Power Management** tab.
   c. Clear the **Allow the computer to turn off this device to save power** check box.
3. Close the **Network Connections** window.
Configuring the CPE 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 10.
- 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 CPE MAS. You must install the Modular Messaging Configuration wizard (MMCW) to configure each CPE MAS.

Complete the following to configure the CPE MAS server using Modular Messaging DCT:

1. Insert the 'Avaya Modular Messaging R5.0 MAS Application DVD 1 of 2' disk into the DVD drive of the CPE MAS server.
2. Navigate to the `Install\MISCM` directory and double-click the `MMConfigurationWizard.msi` file. Do not select the check box that launches the Modular Messaging configuration wizard.
   
   The system installs the configuration wizard in the `C:\Program Files\Avaya Modular Messaging\Install\MISCM` directory and launches the Modular Messaging configuration wizard.
3. Click Finish.
4. Copy the `MMDCT.exe` file from your storage device to `C:\Program Files\Avaya Modular Messaging\Install\MISCM` directory.
5. Run `C:\Program Files\Avaya Modular Messaging\Install\MISCM\MISCM.exe`.
   
   The system opens the Modular Messaging DCT Tool window.
6. On the Modular Messaging Welcome screen, click Next.
7. 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.

8. On the Locate Configuration Data screen, click Next.

9. When the system prompts you to confirm the data file, click Yes. The system opens Avaya Modular Messaging Data Collection Tool window.

10. Click complete and save the data file to the storage device, even if no changes were made. The system returns you to the Avaya Modular Messaging Configuration Wizard.

11. On the Messaging Application Server Number screen:
   a. Change the MAS number field to show the correct number for this server.
   b. Click Next.

12. When the system prompts you to log in, log in to the CPE MAS using the administrator account.

13. When the configuration wizard prompts you to locate the Dialogic installation file, insert the 'Modular Messaging R5.0 MAS Application DVD 1 of 2’ disk.

   Note: The configuration wizard prompts you for the Dialogic installation file only if you install the Dialogic port boards on the CPE MAS.

14. Navigate to the DVD drive and double-click the Dialogic_Drivers\MMDialogicInstall.bat file. The system opens the Dialogic driver installation wizard.
   a. Click Next and accept the licence agreement.
   b. Click Next. Repeat this step until the system displays the Choose Destination Location screen.
   c. Click Browse.
   d. On the Choose Folder screen in the Path: field, change the drive letter to match the drive where Modular Messaging is being installed. This drive is set in the DCT file. Do not browse to find the new location. The path will read <drive letter>:\Program Files\Dialogic.
   e. Click Next and continue to accept default values to complete the wizard.
   f. The system launches the Found New Hardware Wizard. Complete the wizard to install the Dialogic driver software.
   g. When the system prompts you to use Windows update, select No, not at this time and click Next.
   h. When the system prompts you to choose the software, select Install the software automatically and click Next.
i. When the **Security Alert - Driver Installation** window opens, select **Yes** to install the driver.

j. Click **Finish**.

k. Repeat steps f to k for each Dialogic board on this MAS.

l. When the system prompts you, in the **Setup Complete** dialog box, select **No, I will restart my computer later**, and click **Finish**.

15. On the **Remote Shutdown** dialog, click **Cancel**.

16. When the configuration wizard prompts you to locate the **InstallRSEngine** file, insert the ‘Modular Messaging R5.0 MAS Application DVD 2 of 2’ disk.

17. Navigate to the `<drive>\RealSpeak\InstallRSEngine.bat` file and double-click. The system opens the RealSpeak 4.0 InstallShield Wizard.

   a. On the RealSpeak 4.0 InstallShield Wizard, and click **Next**.

   b. Select **I accept the terms in the license agreement**.

   c. Click **Next**. Repeat this step until you see **Change Current Destination Folder** screen

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

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

   f. After the installation is complete, click **Finish**.

   g. When the system prompts you, click **Yes** to restart the system.

      After the machine restarts, Modular Messaging Configuration Wizard launches automatically, the system starts the installation of the RealSpeak languages automatically and displays the status of installation of each language.

   h. Remove the ‘Modular Messaging R5.0 MAS Application DVD 2 of 2’ disk.

18. When prompted for **Setup.exe**, insert the ‘Modular Messaging R5.0 MAS Application DVD 1 of 2’ disk and double-click `<drive>\Install\Setup.exe`.

   The configuration wizard continues the installation of the Modular Messaging MAS components. After the installation of the MM components, the server reboots automatically and MM MISCM continues to run.

19. If JRE is installed during the system upgrade, the system may display ‘Revocation information for the security certificate for this site is not available’. Do you want to proceed?’ message. Click **Yes** to continue.

20. On the WSO configuration wizard, click **Next** and click **Finish**.

   These steps do not complete the configuration of the CPE MAS. To complete the configuration, you must proceed with the next sections.

---

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Completing the CPE MAS configuration

Perform the following tasks to complete the configuration of the CPE MAS:

- **Entering the RAS IP addresses on CPE MAS** on page 98
- **Setting logging location** on page 98
- **Installing anti-virus software** on page 99
- **Configuring the port boards** on page 99

Entering the RAS IP addresses on CPE MAS

Remote access to the server allows the 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.

The Avaya Modular Messaging Configuration Wizard automatically sets up 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. Perform the steps described in **Entering RAS IP addresses on each MAS** on page 50, to set up IP addresses on each MAS to allow remote access.

Setting logging location

⚠️ **CAUTION:**

Ensure that you have adequate space on the drive where your logs are located. If you do not have adequate space, your system may fail to operate correctly.

You may want to change the default location for recording logs when you:

- do not have adequate space on the default C: drive location.
- want to record logs in the same location where you installed Modular Messaging software.

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**.

Close all windows.

---

**Installing anti-virus software**

You must install and administer the anti-virus software as described in **Installing and administering anti-virus software** on page 48.

---

**Configuring the port boards**

*Do this task only if you do not use SIP, H.323 or QSIG.*

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Configuring a customer-provided MAS

Configure the port boards as described in Configuring port boards and switch integration on page 75.

---------------

Continuing with CPE MAS configuration

To complete the configuration of the CPE MAS use the following steps:

1. Continue with Configuring the voice mail system on page 53 through Verifying Audit service on page 83.

2. Continue the installation as appropriate:
   - If you have additional MASs or the supplementary server to configure, repeat the tasks in this chapter for the next MAS through Continuing with CPE MAS configuration on page 100.
   - If all MASs and the supplementary server (if any) is now configured, continue with Chapter 5: Completing initial MSS administration on page 101.
Chapter 5: Completing initial MSS administration

This chapter describes how to complete initial administration on the Message Storage Server (MSS), and how to administer test subscribers for acceptance testing. After you configure all MASs in the Modular Messaging system, you must return to the MSS to complete the basic messaging administration. You can then set up test subscribers, either using a DCT data file or manually, for the system-wide acceptance tests. The amount of administration that you must do on the MSS depends on the optional features that the customer has chosen.

**Note:**

Before you can do the tasks described in this chapter, you must have completed the tasks in Configuring the Avaya MAS on page 41 for Avaya-provided MAS or Configuring a customer-provided MAS on page 85 for a CPE MAS.

Topics in this chapter include:

- Continuing the MSS configuration using a DCT data file on page 102
- Continuing the MSS configuration manually on page 103
- Configuring the MSS modem on page 115
- Installing any software updates on page 116
- Verifying network adapters and bindings on page 116
Continuing the MSS configuration using a DCT data file

This topic explains how to continue the automatic configuration of the MSS using a DCT data file:

1. Log onto the MSS as **craft**; see [Logging on to the MSS](#) on page 22.
2. From the Server Administration menu on the Messaging Administration web interface, click **Configure Using DCT**.
   
   The system displays the configuration information from the DCT data file.
3. Click ONE of the following:
   
   ● If the configuration information is correct, click **Continue Configuration** and continue with the next step.
   
   **Important:** If you click **Fresh Configuration**, as explained below, you will also have to reconfigure each MAS.
   
   ● If the configuration information is incorrect, you must change the information using the DCT file (return to a Windows computer, change the information in the DCT file and copy the file to the storage device) and click **Fresh Configuration**. See the DCT online help for information about changing the DCT data file. If you have to change the DCT data file you must configure the MSS from the beginning; see [Starting the MSS configuration using a DCT data file](#) on page 24.
   
   If you are unable to make the necessary corrections, contact support.
4. On the pop-up screen, click **OK** to continue the configuration.
   
   The page displays the status of the configuration, automatically refreshing the information until the configuration is complete.
5. After the MSS configuration is successfully completed, complete the following:
   
   a. Click **Reboot the system before proceeding**.
   
   b. On the **Reboot Server** page, click **Reboot**.
   
   c. On the pop-up screen that appears, click **OK**.
   
   d. Proceed with [Configuring the MSS modem](#) on page 115.
Continuing the MSS configuration manually

If you chose to configure the MSS manually, this section explains how to complete the configuration. If you chose to configure the MSS using a DCT data file, see Continuing the MSS configuration using a DCT data file on page 102:

- Updating MAS host information on page 103
- Placing the MSS in a Windows domain on page 108
- Administering classes of service on page 110
- Administering special mailboxes on page 112
- Adding test subscribers on page 114

Updating MAS host information

Continue to do the appropriate procedures:

- If using a private Windows domain, proceed with Updating MAS host information in a private Windows domain on page 103.
- If using a corporate Windows domain, proceed with Updating MAS host information in a corporate Windows domain on page 106.

Updating MAS host information in a private Windows domain

*If the MM system uses the corporate Windows domain, see Updating MAS host information in a corporate Windows domain on page 106.*

Updated MAS host information must be sent to each server in the Modular Messaging system:

1. On the Messaging Administration web interface, click Server Administration > MAS Host Setup.
   
   The system displays the Set Up MAS Host Information page.
2. Select the MAS whose information you want to change, such as MAS1.
3. Click Edit.
4. Update the host information to identify this MAS on the corporate and private networks.
Completing initial MSS administration

⚠️ CAUTION:
Complete the Public fields only if the corporate MAS network connection uses static IP addresses.

Continue as follows for the type of network connection used at this site:
- For corporate MAS connections that use DHCP addressing, continue with Step 5.
- For corporate MAS connections that use static IP addresses, complete the Public fields:
  a. In the Public System Name field, enter the corporate full computer name for the MAS, such as mymas1.loc.avaya.com.
  b. In the Public IP Address field, enter the corporate IP address of the MAS.

⚠️ CAUTION:
Do not enter the MAS Windows NetBIOS (such as mymas1) in the Public Aliases field.

Do not enter same name in two fields. A name must be unique across a TCP/IP Network configuration, External hosts and MAS Host Setup web forms. For example, if a domain qualifier appears in a Public Aliases name, such as mymas1.loc.avaya.com, you must use a different name in Private Aliases, such as mymas1.privdom1.local.

   c. In the Public Aliases field, enter only aliases that the corporate network requires.

      You can enter up to five aliases if required. Any names you enter must be unique on the Modular Messaging system and on the network. Separate each name with a space.

5. For all servers, verify the private LAN information:

⚠️ CAUTION:
Do not change the Private System Name or Address fields for a new system. A change to the private name, or using a private IP address outside of the three allowable ranges, can prevent the system from working. If you must change the private name or use a unique private IP address, contact remote support for the special procedures required to change these values.

   a. Verify that the Private IP Address field shows the correct private IP address range for this site. If required, edit the private IP address for this server to use the right range.
b. In the Private Aliases field, enter the following:

- The private full computer name for this MAS on the private network, such as `mymas1.privdom1.local`.
- If the Public System Name entry includes a domain qualifier, such as `loc.avaya.com`, you must include the MAS Windows NetBIOS name in the Private Aliases field. For example, you must enter `mymas1` as an alias for the corporate computer name `mymas1.loc.avaya.com`.

For example, to complete the Private Aliases field, you would enter the following two names for MAS#1, separated by a space:

`mymas1.privdom1.local  mymas1`

c. For Administrator Login, enter the domain administration account, such as `dom-admin`, and the Administrator Password for the account. The account enables the MAS to accept information updates.

6. Click Save.

7. Repeat the above process for each MAS and the Supplementary server.

8. On the Messaging Administration Web admin page, click Server Administration > MAS Host Send.

   The system displays the Send MAS Information page.

9. Click Send.

   - The system sends the host information to all MASs at the same time and reports whether the information was updated successfully. Verify that all servers in the network are updated. If so, continue with Placing the MSS in the private Windows domain on page 108.

   - If an update to a server failed, check the network operation, using a ping test:
     a. From the Diagnostics menu, click Ping Another Server.
     b. On the ping test page, enter the IP address of the failed MAS.
     c. Click Ping Test to establish connectivity.

   **Note:**
   You must ping by IP address to test the connectivity. The test fails if you ping by name and the MAS host file.

d. Repeat the test, as needed, to isolate the problem.

e. Once the problem is corrected, try to send the host information again.

10. Reboot the MSS; see Rebooting the MSS on page 39.
Completing initial MSS administration

Updating MAS host information in a corporate Windows domain

_If the MM system uses the private Windows domain, see Updating MAS host information in a private Windows domain on page 103._

Each MAS server in the Modular Messaging system must receive updated host information. To update the host information for each MAS:

1. From the Server Administration main menu, click **MAS Host Setup**.
   
   The system displays the **Set Up MAS Host Information** page.

2. Select the MAS whose information you want to change, such as **MAS1**.

3. Click **Edit**.

4. On the **MAS Host Information Setup** page, update the host information to identify the MAS on the corporate and private networks.

   **CAUTION:**

   Complete the **Public** fields only if the corporate network connection uses static IP addresses.

   Continue as follows for the type of network connection used at this site:

   - For corporate connections that use DHCP addressing, continue with Step 5.
   - For corporate connections that use static IP addresses, complete the **Public** fields:
     
     a. In the **Public System Name** field, enter the corporate full computer name for the MAS, such as `mymas1.loc.avaya.com`.

     b. In the **Public IP Address** field, enter the corporate IP address of the MAS.

   **CAUTION:**

   _Do not_ enter the MAS Windows NetBIOS (such as `mymas1`) in the Public Aliases field.

   _Do not_ list the same name in two fields. For example, if a domain qualifier appears in a **Public Aliases** name, such as `mymas1.loc.avaya.com`, you would use a different name in **Private Aliases**, such as `mymas1.privdom1.local`.

   c. In the **Public Aliases** field, only enter aliases that the corporate network requires.

      You can enter up to five aliases if required, that are unique on the Modular Messaging system and on the network. Separate each name with a space.
5. For all servers, verify the private LAN information:

⚠️ **CAUTION:**

*Do not change* the **Private System Name** or **Address** fields for a new system. Changing the private name, or using a private IP address outside of the three allowable ranges, can prevent the system from working. If you must change the private name or use a unique private IP address, contact remote support for the special procedures required to change these values.

a. Verify that the **Private IP Address** field shows the correct private IP address range for this site. If required, edit the private IP address for this server to use the appropriate range.

b. For **Private Aliases**, if the Public System Name entry includes a domain qualifier, such as *loc.avaya.com*, you must include the MAS Windows NetBIOS name in the **Private Aliases** field. For example, you must enter *mymas1* as an alias for the corporate computer name *mymas1.loc.avaya.com*.

c. For **Administrator Login**, enter the customer account, such as *custacct*, and the **Administrator Password** for this account. This account enables the MAS to accept information updates.

6. Click **Save**.

7. Repeat the above process for each MAS.

8. From the **Server Administration** menu, click **MAS Host Send**.

   The system displays the **Send MAS Information** page.

9. Click **Send**.

   - The system sends the host information to all MASs at the same time and reports if the information was updated successfully. Verify that all servers that are currently in the network are updated. If so, continue with Placing the MSS in the corporate Windows domain on page 109.

   - *If an update to a server failed*, check the network operation, using a ping test:

     a. From the **Diagnostics** menu, click **Ping Another Server**.

     b. On the ping test page, enter the IP address of the failed MAS.

     c. Click **Ping Test** to establish connectivity.

   **Note:**

   You must ping by IP address to test connectivity. The test fails if you ping by name and the MAS host file.

   d. Repeat the test, as needed, to isolate the problem.

   e. Once the problem is corrected, try to send the host information again.

10. Reboot the MSS; see Rebooting the MSS on page 39.

---

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Completing initial MSS administration

---

Placing the MSS in a Windows domain

Continue to the appropriate procedures:

- If using a private Windows domain, continue to Placing the MSS in a Windows domain on page 108.
- If using a corporate Windows domain, continue to Placing the MSS in the corporate Windows domain on page 109.

Placing the MSS in the private Windows domain

If the MM system uses the corporate Windows domain, see Placing the MSS in the corporate Windows domain on page 109.

You must add the MSS to the private Windows domain that you set up on MAS#1. To do this task, you must have completed Updating MAS host information in a private Windows domain on page 103.

To add the MSS to the private Windows domain:

1. From the Server Administration menu, click **Windows Domain Setup**.
   
The system displays the Set Up Windows Domain page.
2. Ensure that you clear the **Use Corporate LAN?** check box.

   **Note:**
   
The **Kerberos Realm** and **Authentication Method** fields are disabled for private Windows domain.

3. Enter the following information in each field:

   a. For **MSS NetBIOS Name**, type the MSS private system name, which is *mss1*.
   b. For **NetBIOS Domain Name**, type the NetBIOS domain name for the private Windows network that was created on MAS#1, such as *privdom1*.
   c. For **Fully Qualified Domain Controller Name**, type the full computer name for MAS#1 on the private network, such as *mymas1.privdom1.local*.
   d. For **Account for Joining The Domain** using a private Windows domain, enter the domain administrator login, such as *dom-admin*. This account enables the MAS to accept information updates.
   e. For **Password for Joining the Domain**, type the password for the account to the domain you used in step 3d.
4. Click **Save**.
   
The page displays the Windows domain setup status.
Placing the MSS in the corporate Windows domain

*If the MM system uses the private Windows domain, see* [Placing the MSS in the private Windows domain on page 108.](#)

You must add the MSS to the corporate Windows domain. To do this task, you must have completed [Updating MAS host information in a corporate Windows domain](#) on page 106.

To add the MSS to the corporate Windows domain:

1. From the Server Administration menu, click **Windows Domain Setup**.
   
   The system displays the Set Up Windows Domain page.

2. Ensure that the **Use Corporate LAN?** check box is checked.

3. Enter the following information in each field:
   
   a. For **Authentication Method**, select default, Winbind or Kerberos from the list as appropriate.
      
      By default, the system uses Winbind access method.
   
   b. If you have selected Kerberos in step 3a, for **Kerberos Realm**, enter the fully qualified Kerberos Realm name.
   
   c. For **MSS NetBIOS Name**, type the Host Name.
   
   d. For **NetBIOS Domain Name**, type the NetBIOS corporate domain name for the corporate Windows network, such as `loc`.
   
   e. For **Fully Qualified Domain Controller Name**, type the full computer name of the corporate network.
   
   f. For **Account for Joining the Domain** using a corporate Windows domain, enter the customer account, such as `custacct`. This account enables the MAS to accept information updates.
   
   g. For **Password for Joining the Domain**, type the password for the account to the domain you used in step 3f.

4. Click **Save**.

   The page displays the Windows domain setup status.
Completing initial MSS administration

Administering classes of service

You must administer classes of service for the special mailboxes, such as postmaster or fax, and for all test subscribers.

- Setting up a cos for required special mailboxes on page 110
- Setting up a cos for test subscribers on page 111

Setting up a cos for required special mailboxes

Set up a unique class of service (cos) for the special mailboxes. Special mailboxes include the required postmaster mailbox and the optional fax mailbox, if the fax service is installed.

To set up a class of service for the special mailboxes:

1. From the Messaging Administration web interface, click **Classes-of-Service**.
   - The system displays the Manage Classes-of-Service page.
2. Select the class of service to modify, such as **class00**.
3. Click **Edit the Selected COS**.
4. On the Edit a Class-of-Service page, change the **Class of Service Name** to a descriptive name, such as **SpecialMailbox**.
5. In the **MAILBOX AND MESSAGE SIZES** section:
   a. Change the units for **Maximum Mailbox Size** to **Mbytes**
   b. Enter **64** to change Maximum Mailbox Size to **64 Mbytes**.
6. In the **SUBSCRIBER FEATURES AND SERVICES** section, activate the following features:
   
   ![CAUTION:](image)
   - Set MWI for special mailboxes to **No**. Otherwise, system performance is affected.
   a. Set **Message Waiting Indication Allowed** to **no**.
   b. Set all supported notification options to **yes**. For example, set Call Me, Find Me, and Notify Me to **Yes**.
   c. To access a mailbox using a desktop client, set **Restrict Client Access** to **No**. Desktop clients include the Microsoft Outlook client and the IBM Lotus Notes client.
7. Click **Save**.
   - The system displays the Manage Classes-of-Service page.
Setting up a cos for test subscribers

Set up a unique class of service (cos) for each telephone user interface (TUI) that this Modular Messaging system supports. To set up classes of service for the test subscribers:

1. On the Manage Classes-of-Service page, select the class of service to modify, such as class01.
2. Click Edit the Selected COS.
3. On the Edit a Class-of-Service page, change the Class of Service Name to a descriptive name, such as AriaTUI.
4. Scroll down to the SUBSCRIBER FEATURES AND SERVICES section. Activate the following features:
   a. Leave Message Waiting Indication Allowed set to yes.
   b. Set all supported notification options to yes. For example, set Call Me, Find Me, and Notify Me to yes.
   c. If fax service is required, set Outbound Fax Calls to yes.
   d. Set Record Mailbox Greetings to yes.
   e. To access the mailbox, set Restrict Client Access to no. Mailbox clients include the Microsoft Outlook client and the IBM Lotus Notes client.
   f. For Telephone User Interface, select the interface required for this class of service. TUI interfaces include MM Aria, MM AUDIX, and MM Serenade.
5. Click Save.
6. To set up another class of service, repeat Steps 1 through 5. For example, you might set up a class of service for each type of telephone user interface, such as AudixTUI or SerenadeTUI.
Completing initial MSS administration

Administering special mailboxes

You must set up a postmaster mailbox on each system, or the system will fail to work. If fax service is to be installed, you must also set up the required fax service mailbox.

To set up the required mailboxes:

1. Set up the required Postmaster Mailbox.

Note:

Usually you set up a special mailbox to act as the Postmaster Mailbox. Because this mailbox is required for the system to function properly, it should not be a mailbox likely to be deleted or have changes made to it. It will, however, have administrative messages delivered to it upon occasion and should be checked regularly (on a daily basis if possible).

a. From the Messaging Administration web interface, click Messaging Administration > Subscriber Management. The system opens Manage Subscribers page.

b. Next to the Local Subscriber Mailbox Number field, click Add or Edit.

c. On the Add Local Subscriber page, enter the following information:

1. For Last Name, type postmaster. Use lower-case letters.

2. Leave First Name blank.

3. For Password, type the password for the postmaster mailbox.

4. For Mailbox Number, type a valid mailbox number. Enter 3-to-10 digits as required by the dial plan.

5. For Numeric Address, type an address that is unique for the messaging network. The numeric address can be identical to the Mailbox Number, or you can alter them to facilitate easier addressing by remote subscribers. For example, you might prepend a 1 or the area code to the mailbox number.

6. For Class Of Service, select the cos that you set up for special mailboxes. See Setting up a cos for required special mailboxes on page 110.

Note:

The Email Handle will be auto populated when you save this information. It must be postmaster in lower-case letters. Any other email address causes an error. All fields in the SUBSCRIBER DIRECTORY will also be saved.

2. Scroll down and click Save.

3. At the confirmation prompt, click OK.
4. If fax service is installed, set up the required fax service mailbox.

   **Note:**
   The IP H.323 switch integration does not support fax service.

On the Manage Subscribers page:

a. Click **Add or Edit**.

b. On the **Add Local Subscriber** page, enter the following information:
   1. For **Last Name**, type **fax**.
   2. For **Password**, type the password that was entered in the DCT data file.
   3. For **Mailbox Number**, type a valid mailbox number. This is the same mailbox number that you configured earlier on the MAS; see page 32.

   **Note:**
   This number must not be a real telephone (PBX) extension on the system, or the fax feature will not work correctly.

4. For **Numeric Address**, type an address that is unique among all the addresses in the messaging network. The numeric address can include or be identical to the **Mailbox Number**.

5. For **Class Of Service**, select the cos that you set up for special mailboxes. See [Setting up a cos for required special mailboxes](#) on page 110.

c. Scroll down and click **Save**.

d. At the confirmation prompt, click **OK**.

5. From the Messaging Administration web interface, select **Messaging Attributes**.

The system displays the Configure Subscriber Management page.

a. In the **SYSTEM MAILBOXES** section:
   1. For the **Internet postmaster Mailbox Number**, enter the extension for the Mailbox Number that you used in Step 1.
   2. If fax is installed, for the **Fax Mailbox Number**, enter the extension for the Mailbox Number that you used in Step 4.

b. Scroll down and click **Save**.

---

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

Set up at least one local subscriber to test the system. If you have to test multiple types of telephone user interface (TUI), set up a test subscriber for each TUI. For instructions on how to add and configure the mailbox, see the Avaya Modular Messaging MAS Administration Guide.

To add test subscribers:

1. From the Manage Subscribers page, next to the Local Subscriber Mailbox Number field, click Add or Edit.

   The system displays the Add Local Subscriber page.

2. Fill in the fields in the Subscriber Information section as shown in Table 6: Subscriber page sample settings. Click Help if you need more information about completing any fields on this page.

3. Scroll down and click Save.

4. At the confirmation prompt, click OK.

5. If you want to test multiple user interfaces, repeat Steps 1 through 4 to set up an MM AUDIX or MM Serenade test subscriber, as required.

Table 6: Subscriber page sample settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>Aria</td>
</tr>
<tr>
<td>First Name</td>
<td>Test</td>
</tr>
<tr>
<td>Password</td>
<td>1</td>
</tr>
<tr>
<td>Mailbox Number</td>
<td>Type a valid number for the test subscriber mailbox. Usually this is the same number as the primary telephone (PBX) extension for that subscriber. Enter 3-to-50 digits as required by the dial plan.</td>
</tr>
<tr>
<td>Class of Service</td>
<td>Use the one you modified for Setting up a cos for test subscribers on page 111, or as directed. It must have all the features that you need to test activated.</td>
</tr>
<tr>
<td>Numeric Address</td>
<td>Type an address that is unique within the messaging network. The numeric address can include or be identical to the Mailbox Number. Enter 3-to-50 digits as required by the dial plan.</td>
</tr>
</tbody>
</table>
Configuring the MSS modem

To configure the optional USB modem on the MSS, complete the following:

**Note:**
Configure the USB modem only after you have physically connected the modem.

1. From the Messaging Administration web interface, on the Server Administration menu, click **Modem/Terminal Configuration**.

2. On the Configure Modem/Terminal page, locate the correct modem either inside the **Serial Modems and Terminals** box or the **USB Modem** box. For a serial modem you need to know if it's connected to COM1 or COM2. For a USB modem, the "USB Modem Connected?" column will be marked **YES**.

3. From the Modem Type drop-down menu, select the type of modem you are use. If you select Other, you will need to fill in the Modem Init String.

4. From the Speed drop-down menu, select the applicable speed of the modem.

5. Click the checkbox in the far-left column for that modem, click **Save**.

Configuration status displays "successfully registered."
Installing any software updates

A new Modular Messaging system ships with the most current software that is available at the time. However, you must update the software 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.

Complete the following steps to update Modular Messaging software:


   Note: If you followed the procedure for Downloading software updates on page 10, you already downloaded any required software updates.

2. Complete the update procedure before you do acceptance testing:
   a. Follow the instructions provided in Appendix E: Updating Modular Messaging software on page 323 to update the system with the latest changes.
   b. After you install the updates, continue with Chapter 6: Performing acceptance tests for a new installation on page 117.

Verifying network adapters and bindings

After you install an Avaya S8730 MAS or a Supplementary server, complete the following steps to verify the search order in which private and corporate LANs are ordered on an MAS or a Supplementary server.

2. Right-click and select Properties. The system opens the Network Connections window.
3. From the Advanced menu, click Advanced Settings.
4. In the Adapters and Bindings tab, from the list of connections, ensure that the connection to the private LAN (Local Area Connection) appears above the connection to the corporate LAN (Local Area Connection 2). This is to ensure that MAS accesses private LAN before the corporate LAN.

   Note: If the Local Area Connection is not the first entry, select Local Area Connection. Use the up arrow key to move the item to the first position. Click OK.

5. Close all open Windows.
Chapter 6: Performing acceptance tests for a new installation

This chapter describes how to run acceptance tests for each Messaging Application Server (MAS) that is set up to take calls. Acceptance tests verify that the Modular Messaging system is working correctly. You can run these tests from any MAS.

⚠️ CAUTION:

You must first install any software updates before performing acceptance tests, see Installing any software updates on page 114 for information.

You must wait about one minute for the MSS and MAS to synchronize their data after you add any test subscribers. Otherwise, the acceptance tests will not run correctly.

Topics in this chapter include:

- Setting up monitoring tools—optional on page 118
- Running acceptance tests on page 120
- Removing the test subscribers on the MSS on page 128

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Performing acceptance tests for a new installation

Setting up monitoring tools—optional

You can use the monitoring tools described in this section to help you complete the acceptance tests.

Using the Operation History Viewer

You can use the Operation History Viewer to monitor the call progress for any MAS. You can also identify the cause for the problems that occur during testing.

Note:
Without additional configuration, the Operation History Viewer will function on the server only where the Tracing Service is running. For more information about using the Operation History Viewer, obtain the Avaya Modular Messaging MAS Administration Guide; see Downloading user documentation on page 12.

To open the Operation History Viewer:

1. Click Start > Programs > Avaya Modular Messaging > Operation History Viewer.
2. Set up a live mode session for all MASs in the voice mail domain:
   a. In the Operation History Viewer window, click File > New.
   b. In the Session Properties window, verify that Message Application Server shows All Servers.
   c. Select Live Mode check box.
   d. Verify that all the Select Types check boxes are selected.
   e. Under Selection Activities, verify that All Activities check box is selected.
   f. Click OK.
3. During testing, monitor Operation History (OPH) events in the OPH Viewer. The OPH Viewer displays events as they happen on the system.
4. After testing is complete, close the OPH Viewer.
5. If the system prompts you to save the session, click No.
Setting up monitoring tools—optional

Setting up the port monitor

Test calls come in through the ports on various MASs in the system depending on how the hunt group is set up on the PBX. Use the port monitor to verify that the test calls you make come in through the ports of the MAS that you want to test.

To display the port monitor:

1. Switch the monitor to show the correct MAS. For more information, see Displaying an MAS from the console on page 42.
2. Click Start > Programs > Avaya Modular Messaging > Port Monitor.
3. When the system prompts for the Message Application Server, select the MAS that you want to test, such as mymas2. Click Select.
   The Port Monitor displays the ports for this MAS.
4. Repeat Steps 1 through 3 to bring up Port Monitor windows on multiple MASs if desired.
5. After you dial the message retrieval number for the Modular Messaging system during the acceptance tests, check the Port Monitor window.
   - Verify that the call is coming in on a port of the MAS that you want to test.
   - If you notice that the test call does not come through the desired MAS, hang up. Dial the message retrieval number again, until you reach the correct MAS.

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. Alternatively, the hunt group might be administered to send all the calls to one MAS before it sends any calls to a subsequent MAS.
Performing acceptance tests for a new installation

---

**Running acceptance tests**

Test each MAS that is set up to handle calls.

---

**Leaving a call answer message**

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

To place a test call that can be answered by the Modular Messaging system:

1. Call the first test subscriber extension from another telephone. Use an extension for which you have access to the physical telephone. Allow the Modular Messaging system to answer.

2. Speak into the telephone and record test message after the tone, for example:
   "This is a test call answer message."

3. Hang up the telephone to disconnect.

4. If you have to test multiple telephone user interfaces, repeat steps 1 through 3 to leave a call answer message for the next test subscriber.
Retrieving test messages in integrated mode

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

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 telephone.

**Note:**

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

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

a. Verify that the Mailbox Monitor and MWI services are started on the server designated as the MWI server (and on no other server).

b. Verify that the Mailbox Monitor and MWI services are started:

   1. Double-click the **Monitor** icon on the desktop of the MAS designated as the MWI server, and then scroll down to these MM services in the right pane.

   2. If the Mailbox Monitor or MWI service is stopped or if the **Status** column is blank, right-click the appropriate MM service and select **Start**.

   3. Close this window.

c. If the Mailbox Monitor and MWI services are started, check for any problem in the following:

   - test subscriber administration. MWI service **must** be enabled both in the **Class of Service** and in **Subscriber Options** for the subscriber.
   - switch integration
   - switch number administration for the test telephone

2. From the test subscriber telephone, dial the message retrieval number for the Modular Messaging system.

3. Enter the password for this mailbox and press the pound key (#).

   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.
Performing acceptance tests for a new installation

5. After the mailbox is set up, retrieve the test message.

The system uses different commands to retrieve messages, depending on the type of user interface you use. Continue with the appropriate user interface:

- On the MM Aria interface:
  a. Press 11 to review the new voice messages.
  b. Listen to the test message. If the message does not play properly, contact the remote support center.
  c. Press 7 to erase this message.
  d. Repeat Steps b and c to review the next message, if any.
  e. Press the star key (*) to return to the main menu.
  f. Continue with Step 6.

- On the MM AUDIX interface:
  a. Press 2 to review the new messages.
  b. Press 0 to listen to the test message. If the message does not play properly, contact the remote support center.
  c. Press star (*) D, or star (*) 3, to erase this message.
  d. Repeat Steps b and c to review the next message, if any.
  e. Press star (*) R, or star (*) 7, to return to the main menu.
  f. Continue with Step 6.

- On the MM Serenade interface:
  a. Press 5 to review the new messages.
  b. Listen to the test message. If the message does not play properly, contact the remote support center.
  c. Press 3 to erase this message.
  d. Repeat Steps b and c to review the next message, if any.
  e. Press the pound key (#) to return to the Ready menu.

6. Hang up the telephone to disconnect.

7. 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.
Creating and sending a test message in nonintegrated mode

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

Use the following steps to create and send a test message in nonintegrated mode:

1. Dial the message retrieval number for the Modular Messaging system from any telephone that is not administered on the system.
   The system voices the "Welcome to Avaya Messaging" prompt.
2. Press the pound key (#) to skip the system introduction.
3. Enter the extension number for test subscriber mailbox.
4. Enter the password for this mailbox and press the pound key (#).
   The system voices the name of the test subscriber.
5. To create a new voice message:
6. Speaking into the telephone, record the following or a similar test message after the tone: "This is a test voice mail message."
7. Press the pound key (#) to approve the message.
8. When the system prompts you for the mailbox number, enter the mailbox number of another test subscriber. Then press the pound key (#).
   The system voices the name of the test subscriber.
9. To approve the message and address list:
   - On the MM Aria interface, press the pound key (#) twice.
   - On the MM AUDIX interface, press the pound key (#).
   - On the MM Serenade interface, press the pound key (#) twice.
10. Press the pound key (#) again to send the test message to the test subscriber mailbox.
11. Hang up the telephone to disconnect.
12. Retrieve the message as described in Retrieving test messages in integrated mode on page 121.
Performing acceptance tests for a new installation

---

**Testing the outcalling capability**

Test the outcalling capability of the system:

To test system outcalling:

1. Switch the monitor to show the appropriate MAS. For more information, see [Displaying an MAS from the console](#) on page 42.

2. Run the Modular Messaging Client software:
   a. On the Avaya MAS, open **Internet Explorer**.
   b. If the system displays a warning that the Internet Explorer Enhanced Security Configuration is enabled, click **OK**.
   c. In the Internet Explorer main window, select **Tools > Internet Options**.
   d. In the Internet Options window, click the **Security** tab.
   e. Click **Trusted Sites** so the item is highlighted, and then click the **Sites** button.
   f. In the Trusted sites window, verify that the **Require server verification (https:) for all sites in this zone** check box is clear.
   g. Under **Add this Web site to the zone**, enter the full corporate computer name of the MSS and click **Add**. Use the format `mymss.loc.avaya.com`, for example, enter `mss.dr.avaya.com`.

   ! **Important:**

   Do not enter `http://` or `https://` in front of the computer name, or the browser might not find the server automatically.

   h. Click **OK** to close the Trusted sites window.
   i. Click **OK** to close the Internet Options window.
   j. In the address field of the Internet Explorer main window, enter `http://mss1`, the private address of the MSS and then press **Enter**. Use the format `mymss.loc.avaya.com`, for example, type `mss.dr.avaya.com`.

   k. Continue logging in to the MSS.

3. Launch Subscriber Options:
   a. On the **Messaging Administration** web interface, Click **Messaging Administration > Subscriber Management**.
   b. On the **Manage Subscribers** page, type a mailbox number into the **Local Subscriber Mailbox Number** field and click **Add or Edit**.
   c. On the **Edit Local Subscriber** page, scroll to the bottom of the page and click **Launch Subscriber Options**.
   d. On the File Download window, click **Open**.
4. Set up the recording and playback options to use a telephone near you:
   a. In the Modular Messaging User Properties window, click the **Media Setup** tab.
   b. For **When composing voice messages**, select **Telephone**.
   c. Click **Configure**.
   d. In the Telephone Properties window, enter the extension number of a telephone near you.
   e. Select or enter the name of this MAS if needed. Click **OK**.
   f. For **When reviewing voice messages**, select **Telephone**.
   g. Repeat Steps c through e to set up telephone playback.
   h. Click **Apply**.

5. Record a personal greeting:
   a. In the Modular Messaging User Properties window, click the **Greetings** tab.
   b. Verify that system will use the telephone to record 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 Rules:
      1. Under Default call handling, select **Play my personal greeting**.
      2. Click red **Record** button on the player near the bottom of the window.
      3. When the telephone rings, answer the call and record a personal greeting for the test subscriber.
      4. After you record the test greeting, hang up the phone.
      5. Click **Apply**.
Performing acceptance tests for a new installation

6. Play back the greeting to test outcalling, as follows:
   a. Click the black, single-arrow **Play** button on the player near the bottom of the window.
   b. Answer the telephone when it rings.
      The picture of the telephone changes to off-hook.
   c. Listen for the system to play the greeting of the test subscriber.
   d. Hang up the telephone.
      The picture of the telephone changes back to being on-hook in two seconds.

7. Set up the MWI rule:
   a. On the Assistant tab, right-click Message Waiting Indicator and select **New Rule**. Make sure that the option is checked.
   b. Click the Message Waiting Indicator rule that appears. Text for the rule appears near the bottom of the tab.
   c. Click **Apply**.

8. Click OK to close the Modular Messaging User Properties window.

9. Close all open windows.
Creating and printing a fax message

Do this test only under the following circumstances:

- When the MM Fax Sender server is installed in the vmd.
- On the MAS that hosts the MM Fax Sender server.

To create and send a test fax message:

1. From a fax machine, send a fax to the test subscriber mailbox. The subscriber's class of service must have both Inbound Fax and Outbound Fax Calls set to Yes.

2. Wait a few minutes for the fax to be delivered. The MWI lamp, if present, on the test subscriber telephone should light.

3. From a telephone (NOT the fax machine), dial the message retrieval number for the Modular Messaging system.

4. Press the pound key (#) to access the test subscriber mailbox.

5. Enter the extension number for the test subscriber mailbox.

6. Enter the password and press the pound key (#).
   The system speaks the name of the test subscriber.

7. Retrieve and print the fax 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 19 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.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Removing the test subscribers on the MSS

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

1. Switch the monitor to show the MSS.
2. From the Messaging Administration web interface, click **Subscriber Management**.
   The system displays the Manage Subscribers page.
3. On the line **Local Subscribers** for this MSS, such as **mymss**, click **Manage**.
4. On the Manage Local Subscribers page:
   a. Select the test subscriber to delete.
   b. Click **Delete the Selected Subscriber**.
   c. If the system prompts you to confirm removing the subscriber, click **OK**.
   d. At the confirmation prompt, click **OK**.
5. Repeat Step 4 to remove all test subscribers.
Chapter 7: Setting up support and making system backups

This chapter describes how to complete the serviceability configuration for the Message Storage Server (MSS), backup the Modular Messaging system information and complete the new installation on Modular Messaging system.

This chapter includes the following topics:

- [Setting up logins and remote access](#) on page 130
- [Setting up alarming on the MSS](#) on page 133
- [Backing up the system](#) on page 139
- [Completing the installation](#) on page 142
Setting up support and making system backups

Setting up logins and remote access

Set up the required logins and remote access as described in this section. These steps allow a remote service center to dial in to the system for troubleshooting or system maintenance.

Registering the system in ART

You must register the Modular Messaging system through the Avaya Automatic Registration Tool (ART) to obtain the information that is required to complete the installation. The information that you need for installation includes:

- Product identifier (ID) for each MAS, used to identify the server that generates an alarm
- IP addresses to remotely access each server:
  - the tscppp point-to-point protocol (PPP) login on the MSS for Avaya technical support
  - IP addresses that the remote access service (RAS) uses to access each MAS. You can register an MAS to obtain the product ID and IP addresses in advance. For more information about using ART, see your local procedures.

Registering an MSS

The MSS must be running and remote access must be established when you register the server. For example, you can register the MSS first, and continue with the installation.

When you register the MSS, the Avaya expert system dials in and automatically programs the server with the product ID and tscppp IP addresses. The ART registration process reprograms certain system passwords for improved security.

Registering an MAS

You can register an MAS before you install it because the Avaya expert systems do not automatically dial in or program any information on an MAS. You must register each MAS in the system, including the Supplementary server, if present. The registration process populates the customer login and password information in Maestro and provides RAS IP addresses and product IDs for each server.

To register an MAS, call the Product Registration group. The registration group must add the Cust Assigned Login ID and the Cust Assigned Password in the Maestro. The login and password must match the technical support account for you to access an MAS.

After you register each MAS, record the RAS IP addresses in the DCT data file. To enter RAS IP addresses on the MAS, see Entering RAS IP addresses on each MAS on page 50.
Administering logins and passwords

Note:
You can set this up in the DCT. In that case, these logins and passwords should already be configured for all logins except for dadmin (Business Partners). If you use dadmin, complete this procedure.

You must administer logins and passwords for all Modem Dialout-supported systems to support remote maintenance. You can set up any additional required logins, such as the dadmin login that Avaya Business Partners use to administer or maintain the system.

You can set up additional logins either from the console or from another computer on the customer LAN. You can use the craft login to activate dadmin or other required logins and grant permission.

To administer additional logins:

1. From the Security menu, click **Local Administrators**.
   The system displays the Manage Local Administration Accounts page.

2. Select an account, such as sa or vm, and then click **Edit the Selected Admin**.
   The system displays the Edit Local Administration Account page.
   a. From the Local Authentication Enabled? drop-down menu, select yes (if it's not already selected).
   b. For **Password**, enter the appropriate password.
   c. For **Confirm Password**, type the same password.
   d. Click **Save**.

3. Repeat Step 2 for each additional login that you must administer. The logins include:
   - craftppp for technical support remote access
   - dadmin for Business Partners support
   - sa and vm for customer administration

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Setting up support and making system backups

Setting up the PPP server configuration

Perform this task if you need to provide local and remote IP addresses for point-to-point protocol (PPP) remote access because the system does not provide other connectivity, such as through the Internet. Types of login you might administer this way are craftppp or sappp.

**Note:**
You can set this up in the DCT. In that case, this should already be configured. Also, the ART registration process automatically programs the tscp pp login for Avaya remote technical support.

To set up the PPP service on this server:

1. From the Security menu, click **PPP Configuration**.
   The system displays the Configure PPP Users page.

2. For each login account that you must administer, enter the following information:
   a. For **Local IP Address**, type the customer-provided IP address for PPP access through the MSS modem.
   b. For **Remote IP Address**, type the IP address for the remote device that is to connect to this MSS. Either the customer or remote support might provide this IP address.
   c. For **Password**, type the password for the login account.
   d. For **Confirm Password**, type the same password for the login account.

3. Repeat Step 2 for each of the PPP logins that you must set up.

4. After you administer all required logins, click **Save**.
Setting up alarming on the MSS

Complete and test the setup for alarm on the MSS as described in this section.

Specifying MSS alarm origination

Activate alarm origination to enable the appropriate party to receive notification of alarms that occur on the system. This might be a remote service center or a corporate NMS.

To set up alarm origination through the MSS:

1. Clear all alarms. For instructions, obtain "MSS alarms;" see Downloading user documentation on page 12.
2. Insert a labeled, writable DVD-RAM into the DVD drive for the nightly backup.
3. From the Alarming menu, click Alarming Configuration.
   The system displays the Configure Alarms page.
4. Enter the Product ID for the MSS.
   Note: The ART registration process automatically programs the MSS product ID. A valid product ID must be present, or this test will not work.
5. Set the Alarm Origination for the type of alarm used on this system or indicate that alarm is inactive:
   ● Inactive
   ● Modem Dialout
   ● SNMP
   ● Internet
6. Verify that Alarm Suppression is set to INACTIVE. You can use the default settings for Alarm Level and Clear Alarm Notification. For more information about completing each field, click Help.
7. Complete the alarming information for the site:
   - If you selected **Modem Dialout** alarming, enter the **Modem Dialout Destination** telephone number and then click **Save**.
   - If you selected **SNMP** alarming:
     a. Click **Save** on the Configure Alarms page.
     b. From the Alarming menu, select **SNMP Community**.
     c. On the Administer SNMP Community page, click **Add** to add the community you need for SNMP trap destination. If the community already exists, skip to step g.
     d. For **Community**, click the field and enter a community name. This name is used to validate when communicating between the SNMP client and the SNMP server.
     e. For **Apply To**, from the drop-down menu, select either **Traps** or **Both**.
     f. Click **Save**, a window appears if the add was successful.
     g. From the Alarming menu, select **SNMP Trap Destination**.
     h. Click **Add**.
     i. Complete the appropriate fields. For more information about completing each field, see the SNMP Trap Destination setup in the task **Configuring serviceability settings on MAS#1** on page 58.
     j. Click **Save**.
   - If you selected **Internet** alarming:
     a. Click **Save** on the Configure Alarms page.
     b. From the Alarming menu, select **HTTPS Servers**.
     c. On the Administer HTTP Proxy Servers page:
        - If Internet alarming is not using proxy servers, verify the default addresses in both **Destination** fields.
        - If the enterprise network configuration does not pass HTTP, then set Internal alarming to use proxy servers. From the "Enable Customer HTTPS Proxy Servers" drop-down menu, select **Enabled** and then complete both **Proxy Server** fields.
     d. Click **Save**.
Testing alarming origination

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

**Note:**
This test requires the receiving system, either Modem Dialout, SNMP, or Internet, to be set up by the appropriate party and ready to receive alarms.

For more information about setting up SNMP alarming at a site, obtain "Administering SNMP on the MSS;" see [Downloading user documentation](#) on page 12. Do additional SNMP administration beyond the steps in this installation guide after the Modular Messaging system is set up and running.

To test the alarm origination:

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

As a final installation task, you must ensure that the DCT data file for the Avaya Modular Messaging system is complete and current. To do this, you must collect information from each MAS in the system.

To collect current data from each MAS and the Supplementary server, if present:

1. Replace the MMDCT.exe found in C:\Program Files\Avaya Modular Messaging\Install\MISCM with the most current version (see Downloading software updates on page 10). This must be done on each MAS and Supplementary server.

2. Verify that the Modular Messaging system is working correctly and all servers are running.

3. Switch the monitor to show the server to analyze.

   **CAUTION:**
   
   For a new installation, start with MAS#1 and analyze MASs in order: MAS#1 and then MAS#2, and so on.

4. Insert a storage device into the server.

5. In Windows Explorer, navigate to the directory that contains the DCT program. You can find a copy of the DCT executable file in C:\Program Files\Avaya Modular Messaging\Install\MISCM.

6. Double-click the MMDCT.exe file.

7. In the Avaya Modular Messaging Data Collection Tool window, select **Analyze existing system**, and then click **OK**.

8. When the program asks if you want to use an existing DCT file, click **Yes**.

9. In the Open window, click the drop-down list next to **Look in**.

10. Complete ONE of the following:
    - For MAS#1, navigate to the location of the site’s original DCT data file.
    - For subsequent MASs, navigate to the location of the most current DCT data file on the storage device, such as sitefile-analyzed.mmdct.

   **CAUTION:**
   
   For a multiple-MAS system, you must open the same data file that you saved from the previous MAS. Otherwise, the data from the previous server is lost. Do **not** manually enter the data for subsequent servers! Use the DCT to analyze each server in turn. The tool collects some data that does not appear on the DCT screens.

11. Double-click the appropriate data file.
12. On the MM System Analysis screen, use the **MAS Information is being collected from** drop-down menu to select the appropriate MAS, such as **First MAS (#1)** or **Second MAS (#2)**.

13. Click **Start**.

   The system displays the data collection process in the window. After the information is collected successfully, which could take several minutes, the system displays a confirmation window.

14. Click **OK**.

15. On the **Avaya Modular Messaging Data Collection Tool** window, click **Save**.

16. In the **Save As** window, navigate to the storage device.

17. Complete **one** of the following:

   - For MAS#1, type the name of the date file in the **File** name field. Use a new filename to indicate that this is the most current data file. For example, you might type `sitefile-analyzed`.
   - For subsequent MASs, select the same file you saved for MAS#1, such as `sitefile-analyzed`, in the **File** name field.

18. Click **Save**. For subsequent MASs, then click **Yes** when asked if you want to replace this file.

19. On the Avaya Modular Messaging Data Collection Tool window, click **Cancel**.

20. Click **No** when asked to save the current configuration (you already saved the file above).

21. Double-click the icon on the task bar to **Safely Remove Hardware** and follow the prompts to safely remove the storage device.

22. Repeat this task for each subsequent MAS.

23. When you have analyzed all MASs and the Supplementary server:
   a. Get the original DCT file.
   b. Get the analyzed DCT file.
   c. In the analyzed DCT file, enter the values in fields that are not populated by the analyzed DCT file with the data from the original DCT file. Use DCT tool to enter the information.
Setting up support and making system backups

Copying the DCT data file for backup

Once all MAS servers in the voice mail domain have been analyzed, copy the most recent version of the DCT data file from the storage device to the MSS. This is to keep a backup of the data.

To copy the most current DCT data file from the storage device:

1. Insert the storage device into an MAS.
2. Log on to the same account that you used on the Windows Domain Setup page for Placing the MSS in a Windows domain on page 106:
   - In a private Windows domain, use the domain administrator account name, such as dom-admin.
   - In a corporate Windows domain, use the customer account name, such as custacct.
3. Copy the updated DCT data file from the storage device to the \mss1\masbackup location on the MSS.
   a. Click Start > Run. The system opens Run window.
   b. Enter \mss1\masbackup and click OK. The system opens the Windows Explorer window.
   c. Copy the DCT data file to the \mss1\masbackup directory.
4. Remove the storage device from an MAS.
Backing up the system

As a final installation task, back up the information that you administered on the system. Do an attended (manual) backup to save your work and to verify the backup function.

Running backups on each MAS

_Do this task on each MAS._

You must send MAS backup data to the MSS, so it can be backed up with the rest of the system data on DVD-RAM.

To back up the data on each MAS:

1. Switch the monitor to show MAS#1. For more information, see Displaying an MAS from the console on page 42.

2. Log on to the same account that you used on the Windows Domain Setup page for Placing the MSS in a Windows domain on page 106:
   - In a private Windows domain, use the domain administrator account name, such as _dom-admin_.
   - In a corporate Windows domain, use the customer account name, such as _custacct_.

3. To view the scheduled backup program for the MAS, double-click the Scheduled Tasks icon on the desktop.

4. In the Scheduled Tasks window, run an attended backup on this MAS:
   a. Right-click the task named MAS Backup and select Run.

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

      When the backup completes successfully, continue with Step 5.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
b. Optional: To verify if the backup process is successful:
   1. Double-click the Monitor icon on the desktop.
   2. In the left pane, expand Event Viewer (Local), and then click Application.
   3. Refresh the window display periodically until you see the following events.
      - `ntbackup 8009`, **End Verify: The operation was successfully completed.**
      - `ntbackup 8019`, **End Operation: The operation was successfully completed.**

Note:
On MAS#1, the event viewer shows two sets of backup events because the backup program generates two files on the MSS: `MYMAS#1MASSingle.bkf` and `MYMAS#1MASAll.bkf`. The process of backup on subsequent MASs generate only the `MASAll.bkf` file for each MAS, so only one set of backup events is present.

   c. If the backup fails to run, verify the account settings:
   1. Double-click the task MAS Backup to view the properties window.
   2. In the MAS Backup window, click the Task tab. Verify that the account in the Run as field is the correct account that has permissions to run backups manually. If the account is incorrect, you can type the correct value now. For more information, see Placing the MSS in a Windows domain on page 106.
   3. If you change the account, or if you want to verify the password, click **Set password**. In the Set Password window, enter and confirm the password for the required account. Click OK.
   4. Click OK to close the MAS Backup window.
   5. Repeat Step 4-a to run the backup again.
   6. Close the Scheduled Tasks window.
   7. Repeat this procedure for each MAS in the system.
Setting up and running a backup on the MSS

After you have run an attended backup of each MAS, run an attended backup on the MSS now.

Make the first system backup to DVD-RAM.

1. Log on to the MSS server as **craft** using the appropriate password.
   
   The system displays the Messaging Administration web interface.

2. From the Backup/Restore menu, click **Backup**.
   
   The system displays the Backup page.

3. Make a backup of the new Release 5.0 system data:
   
   a. Because the system is not yet in service, you do not necessarily have to stop the voice system.
   
   b. Verify that **Media Type** is set to **DVD-RAM**.
   
   c. Set all the data fields to back up to **Yes**.
   
   d. Click **Start Backup**.
   
   e. If the system prompts you to continue, click **Continue**.
   
   f. The system estimates the number of DVDs that it requires. Verify that you have the correct number of DVDs available. Click **Continue**.
   
   g. When the system prompts you to insert the DVD, click **Continue**.
   
   The system saves the new system configuration to the DVD. Allow about 30 minutes for each DVD.

   **Note:**
   
   If you have not inserted a writable DVD, the system displays the following error message: **Wrong media, Please use DVD-RAM media.**

   h. Follow the prompts on the screen to track and complete the backup process. Scroll to the bottom of the page to see the most recent status messages. The message **FULL-MANUAL BACKUP completed successfully** indicates that the backup is complete.

4. Consult the customer to decide the time and the method used to run the periodic unattended backups of the system data.

   The system supports backups to DVD-RAM or through the customer network using FTP or SFTP. For instructions, obtain "Backing up the MSS;" see **Downloading user documentation** on page 12. For overview information, see **Avaya Modular Messaging Concepts and Planning Guide**.

5. When you are finished, log off from the system.
Completing the installation

Use the following steps to complete the installation of a new system:

- **Installing the client software** on page 142
- **Turning over the system** on page 143

Installing the client software

Install the appropriate client software, which includes the following:

- Modular Messaging Web Client. This software *must* be on its own server and *not* on an MAS or a Supplementary server
- Modular Messaging Web Subscriber Options, if installed on a non-MAS server
- Avaya Modular Messaging Notes Client
- Avaya Modular Messaging Outlook Client, Avaya Modular Messaging Outlook Restricted Client, Subscriber Options.

**Note:**

The *Subscriber Options components* are automatically installed on the MAS as part of Release 5.0. *Do not* manually install or delete any MM Clients, including Subscriber Options, on any MAS. For more information, see the *Avaya Modular Messaging Subscriber Options User Guide* and see [Downloading configuration notes](#) on page 11.

- Mailbox Manager
Completing the installation

Turning over the system

The system is now considered ready for handoff to the customer. Complete the following steps as part of the handoff procedure.

1. Make a copy of the original DCT data file used to configure the new system and the analyzed DCT data file created at the end of the installation.

2. Distribute the copies of DCT data files to the following:
   - Customer
   - Project planner
   - Organization that remotely supports the system
   - Appropriate technical support group

3. Delete the data files from your storage device for security purposes.

4. Advise the customer about the initial administration that was completed. The customer can customize the following:
   a. The feature parameters in the Voice Mail System Configuration (VMSC) program. For more information, see Configuring the voice mail system on page 53.
   b. The method used for automatic (scheduled) system backups. For example, customers might want to implement FTP backup over the LAN instead of using DVD-RAM.
   c. The classes of service to use for subscribers might need to be updated or expanded. For more information, see Setting up a cos for test subscribers on page 109.

5. 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 Downloading user documentation on page 12.

Note:

The system is set up to send alarm information and receive incoming technical support calls. If the customer does not want this service, suppress alarm notification. To suppress the alarm notification, select Suppress alarm notifications on the Serviceability page, in the Voice Mail System Configuration. For more information, see Avaya Modular Messaging MAS Administration Guide.
Setting up support and making system backups
Chapter 8: Upgrading to Modular Messaging Release 5.0 on S3500-family server

This chapter describes how to upgrade to Modular Messaging Release 5.0 from Release 3.x or Release 4.0 running on S3500 server.

Note:
You cannot upgrade from Release 2.0 to Release 5.0 or from S3400 server to S8730 server. Migration is the only way you can move the Modular Messaging system from:
- Release 2.0 to Release 5.0
- S3400 server to S8730 server

For more information on how to migrate the Modular Messaging system, see Migrating to Modular Messaging Release 5.0 on S8730-family server on page 201.

If you are moving the Modular Messaging system to the corporate Windows domain, first complete the entire upgrade, then move the system to the corporate Windows domain. For complete information, see Moving to the corporate Windows domain after upgrade on page 188.

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 181.

Topics in this chapter include:

- Planning for the upgrade from Release 3.x or Release 4.0 on page 146
- Performing pre-upgrade tasks on page 150
- Upgrading the MSS from Release 3.x or Release 4.0 on page 166
- Upgrading an MAS from Release 3.x or Release 4.0 on page 168
- Completing the upgrade from Release 3.x or Release 4.0 on page 176.
- Converting Supplementary server to run a 0 port MAS on the Supplementary server on page 178
- Changing switch integration on page 181
- Moving to the corporate Windows domain after upgrade on page 188
Planning for the upgrade from Release 3.x or Release 4.0

Consider the requirements to upgrade the Modular Messaging system given in section Upgrade requirements on page 148.

In Modular Messaging Release 5.0, the process that you use to upgrade a Supplementary server is the same process that you use to upgrade the MAS. Upgrade each MAS and then upgrade the Supplementary server.

You must complete the following before you upgrade from Release 3.x or Release 4.0:

1. Assemble and review the required documentation. For more information about how to access these items on the Web site, see Downloading required software and documentation on page 9:
   - Data Collection Tool (DCT). You do not need a DCT data file for an upgrade. However, you must analyze the system to create a DCT file before the upgrade to save any important system information for backup.
   - Upgrade checklists
   - Web Client Installation and Upgrades guide
   - Web Subscriber Options Installation and Upgrades guide.

2. Manually check for the following:
   a. Ensure that there are no errors or warnings on the system.
   b. Resolve major and minor alarms.
   c. Verify that backups are completed.
   d. Verify that the private IP addresses are in the correct range.

   ▶️ Important:
   When you verify the steps e and f, remember that private IP addresses and corporate IP addresses must not use the same subnet.
   e. Verify that private IP addresses are on the same subnet.
   f. Verify that corporate IP addresses are on the same subnet.
   g. Verify that the private name of the MSS is mss1.
   h. Verify that the corporate NetBIOS name is not mss1. For example, the corporate name cannot be mss1.loc.avaya.com.

3. Review product functionality with the customer:
   - Differences that are noticeable to the customer.
   - Known issues; see Product Support Notices (PSNs) on the Avaya support Web site.
   - Rollout plan for new features.
Planning for the upgrade from Release 3.x or Release 4.0

- Security concerns.

4. Coordinate with MMTAC to provide implementation schedule for Tiered Support.
Upgrade requirements

To upgrade a Modular Messaging system, you need:

- Avaya Modular Messaging R5.0.—MSS Application disk, MSS OS disk and MAS Application disks. For more information about these disks, see Table 1: Required Modular Messaging software on page 8.

- To install the Modular Messaging system, get the following before you start the upgrade:
  a. The original DCT file for the system or planning forms for the system that runs on Release 3.x.
  b. The latest analyzed DCT file for the 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 9.
  - The most current copy of the configuration notes for this switch integration.
  - The Avaya Modular Messaging MSS Pre-upgrade and Backup Verification Tool. For more information, see Installing the Pre-upgrade and Backup Verification tool on page 153.
  - Any Avaya software updates required to bring the Avaya Modular Messaging software up to date after an upgrade. Download the required software to a storage device.

- Print the upgrade checklist from Modular Messaging Release 5.0 upgrade and migration checklists on page 265. Use the checklist to track your progress.
Switching the monitor to show the correct server

You must switch the display from one server to another during a system upgrade.

To display the correct server, complete the following steps:

1. Verify that the monitor is showing the MSS.
   - For a 2-port KVM switch, the MSS is connected to one of the computer port.
   - For an 8-port Belkin KVM switch, the MSS usually is connected to the first computer port on the switch. The port is labeled VGA 01.

2. If the monitor displays a different server, toggle the port to show the MSS.
   - To have a 2-port Belkin KVM switch show a different server:
        The LED on top of the Belkin KVM switch starts to blink.
     b. Type the port number on the keyboard. For example, type 1 for port 1.
   - To have an 8-port Belkin KVM switch show a different server:
     a. Gently press Scroll Lock twice within 2 seconds.
     b. Select the server to display using 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 using the keyboard. For example, type 1 for port 1.

For complete user and troubleshooting instructions on KVM switch, see the KVM switch documentation.
Performing pre-upgrade tasks

Perform the following tasks before you upgrade the system:

- **Preparing for the upgrade** on page 150
- **Preparing for the upgrade on the MAS** on page 151
- **Installing the Pre-upgrade and Backup Verification tool** on page 153
- **Running the Pre-upgrade tool** on page 153
- **Completing pre-upgrade tasks** on page 155

Preparing for the upgrade

You must complete the following tasks before you upgrade the system.

1. Download any Avaya software updates required to bring the Avaya Modular Messaging software up-to-date after an upgrade. Download this software to a storage device. See **Downloading software updates** on page 10.

2. As a precaution (this is information you might need later if you need to recover), verify and record the key settings on the MSS and MAS:
   a. Record non-default port groups.
   b. Record RAS IP addresses for each MAS.
   c. Back up Caller Application files on a separate computer.
   d. Record associations for Caller Applications. You will need this for performing a re-association later.
   e. Record SNMP trap destination and community details from the **Serviceability - Voice Mail Domain** window.

3. Obtain and review the 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.

4. Perform this step *only* if you upgrade from Release 3.0.
   a. Verify that the Modular Messaging Release 3.0 system is at least at Service Pack 7 Patch 4, patch MM300704 (which included RFU M7025rf+m (MM300700) and M7025pt+a (MM300704) for the MSS), and installed on both MAS and MSS.
   b. If the system is not at the required SP level, you must update the Release 3.0 system. Use the following steps to verify the service pack and patch installed on the MAS:
      1. Log on to MAS.
      2. Select **Start > Programs > Avaya Modular Messaging**.
      3. Click the **About Modular Messaging** tab.
Performing pre-upgrade tasks

4. This identifies the version of Modular Messaging installed.

5. Click the **Patches** tab.
   
   This identifies which Service Packs and Patches are installed.

   c. Verify the RFU level on the MSS:
      
      1. On the **Messaging Administration web** interface, click **Software Management > Messaging Software Display**.

5. Perform this step *only* if you are upgrading from Release 3.1.

   a. Verify if the MSS has RFU M7040rf+k from Service Pack 4 installed, as explained in subsequent steps. If RFU M7040rf+k is not on the MSS, skip the following step.

   b. To verify RFU level on the MSS, on the **Messaging Administration web** interface, click **Software Management > Messaging Software Display**.

   c. If RFU M7040rf+k is installed on the MSS, remove M7040rf+k:
      
      1. On the **Messaging Administration web** interface, click **Software Management > Software Removal**.

      2. Select **M7040rf+k** and click **Submit**.

      3. On the next page, click **Proceed with removal**.

6. Perform this step *only* if you are upgrading from Release 4.0

   a. Verify that the Modular Messaging Release 4.0 system is at least at Service Pack 3 (which included RFUs M8017rf+h, A6016rf+g, E6016rf+c and U8017rf+b).

   b. If the system is not at the required SP level, update the Release 4.0 system. Use the following steps to verify the service pack and patch installed on the MAS:
      
      1. Log on to MAS.

      2. Select **Start > Programs > Avaya Modular Messaging**.

      3. Click the **About Modular Messaging** tab.

      4. This identifies the version of Modular Messaging installed.

      5. Click the **Patches** tab.

         This identifies which Service Packs and Patches are installed.

   c. Verify the RFU level on the MSS:
      
      1. On the **Messaging Administration web** interface, click **Software Management > Messaging Software Display**.

**Preparing for the upgrade on the MAS**

Complete the following:

1. Switch the monitor to show the correct server; see [Switching the monitor to show the correct server](#) on page 149.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
2. Verify that all messaging servers and services are running.

3. Verify the DCT data file. A DCT data file is not required for the upgrade; however, analyze the system to create one prior to the upgrade to save important system information for backup. For more information, see Using the DCT to analyze the current configuration on page 136.
Performing pre-upgrade tasks

Installing the Pre-upgrade and Backup Verification tool

The Pre-upgrade and Backup Verification tools are packaged together. You install the tools simultaneously. However, you do not run them at the same time. For information on running the tools, see Running the Pre-upgrade tool on page 153 and Running the Backup Verification tool on page 164.

To install the Pre-upgrade and Backup Verification Tool on MSS:

1. From the Avaya Support Web site, click Modular Messaging and then click Installation, Migrations, Upgrades and Configurations.
2. Download the Pre-upgrade and Backup Verification Tool and copy it to a disk.
   
   You cannot copy the file in any sub folders on that disk.
3. At the prompt on the MSS you are upgrading, login as either tsc, craft, or dadmin.
   
   The server displays the Messaging Administration main menu.
4. From the main menu, click Utilities > Software Management > Software Installation.
5. Insert the disk that contains Pre-upgrade and Backup Verification tool.
6. From the Software Installation menu, click CD.
7. On the screen that appears, click Continue this operation without current system backup.
   
   This installation does not affect the service.
8. On the screen that appears, check pubvt.
9. Click Install selected packages.
   
   The installation begins and takes about one minute. You must see a message that the install completed successfully.
10. Click Return to Main.

Running the Pre-upgrade tool

A member of the installation team from Avaya or the business partner uses the Pre-upgrade tool to identify potential pitfalls and to help plan for the upgrade. This tool produces a report that includes:

- The expected number of disks necessary for a complete backup, including all data categories.
- The expected duration of the upgrade.
- An indication of whether the MAS backup files on the MSS are current (or when the MAS last performed a backup of its data to the MSS).
- An analysis of the active alarms and their effect upon the upgrade.

Running the pre-upgrade tool does not affect your service. Run the Pre-upgrade tool twice.
Upgrading to Modular Messaging Release 5.0 on S3500-family server

- First time two or three weeks before the upgrade.
- Second time the day of the upgrade:

Do the following to run the pre-upgrade tool:

1. At the MSS prompt, log in as either tsc, craft, or dadmin.
2. From the Messaging Administration main menu, click Utilities > Pre-Upgrade Information.
   - The Show Last Summary button only appears if someone has run the tool before. Click Show Last Summary to view the previous summary information.
3. Click Start to begin the pre-upgrade tool.
   - The tool takes about two minutes to run and you get the output every 30 seconds to let you know that the tool is still running. If needed, click Abort to stop the tool from running.
4. Review the output information from the tool.
   - Ideally, there will not be any errors and warnings and you can proceed with the upgrade.
5. If you find any errors or warnings, you must resolve them before you continue with the upgrade.
Completing pre-upgrade tasks

Complete the following tasks before you start upgrade to Release 5.0:

1. If not running, start the MSS.

2. Using the latest DCT file or planning form (if you upgrade from Release 3.x), verify the key settings on the MSS and MAS that includes:
   - Switch integration settings
   - Port board settings and extensions
   - Domain information
   - Basic system setup
   - SNMP trap destination and community details from the Serviceability - Voice Mail Domain window

3. On the Messaging Administration web interface, complete the following:
   a. Under the Alarming menu, click Alarming Configuration.
   b. The system opens Configure Alarms page.
   c. In the Alarm Suppression field, click ACTIVE.

4. On the MAS, complete the following steps to record all Personal Operator Schedules. You need this information 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.

5. 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.

6. On each MAS, record the IP addresses for the MAS modems in the remote access service (RAS) group. You must manually re-enter the RAS IP addresses.

7. If the site has Caller Applications, ensure that copies of all editable files are on a separate computer, not the MAS. The data restoration procedure restores only the deployed Caller Applications. The deployed version is not editable; always use the administrator version. Ensure that all editable Caller Applications scripts are in a separate working folder before
the upgrade, such as on the administrator personal computer. Use the Caller Applications editor to see a list of the deployed applications.

8. Review the configuration notes for any changes that might be needed about the board configuration, switch programming, and application configuration. Make any necessary changes as part of the upgrade.

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. The tool copies the server system information into a data file, allowing for easy reconfiguration of the servers.

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.

Collecting DCT data

Use the DCT to collect the system data:

1. Run a DCT analyze on the system, see Using the DCT to analyze the current configuration on page 136.
2. Proceed with Verifying DCT data on page 156.

Verifying DCT data

After analyzing the last MAS to be upgraded, the Avaya Modular Messaging Data Collection Tool (DCT) displays the results of the last analysis. The DCT collects most of the system information. However, you must enter some of the data manually, and verify the information as described in this section.

⚠️ Important:
You must verify the data in the analyzed DCT file only after you have analyzed all MASs and Supplementary servers in your MM System.

For more information about completing the DCT screens, click the Help button in the Avaya Modular Messaging Data Collection Tool window. You can also use the printed document, Avaya Modular Messaging Data Collection Tool Online Help; see Downloading user documentation on page 12.
Performing pre-upgrade tasks

Do not change data that is populated by the DCT.

⚠️ Important:
If the DCT left pane shows a red X for an item, the data is incomplete or incorrect on that screen. Click each flagged item and correct the problem before you continue. Information must be complete and valid to continue with the upgrade. If you cannot fix a bad entry, do not continue with the upgrade.

1. From the DCT window, on the Customer details screen:
   - a. Complete all fields on this screen.
   - b. Click Next.

2. Verify the settings on the Regional settings screen. Click Next.

3. Verify that the message store is MSS with Avaya MAS servers. Click Next.

4. On the Voice Mail Domain screen:
   - a. Verify the name for the voice mail domain (VMD).
   - b. Verify the number of MASs in the voice mail domain.
   - c. Click Next.

5. Verify the corporate network setting. Click Next.

6. On the Corporate MM server networking details screen:
   - a. Verify the server names and other settings, depending on the connection type. If necessary, fill in the IP address and the Full computer name fields.
     The DCT updates this information with each MAS that it analyzes.
   - b. Click Next.

7. On the Corporate network details screen:
   - a. Verify the domain name server (DNS), corporate default gateway, and WINS values. If the WINS field shows 127.0.0.0, change it to the correct value.
   - b. Click Next.

8. On the Private network screen, verify that all the settings are correct. Click Next.


11. On the MSS message store screen, verify that the information matches with your configuration.
    For more information, see Avaya Modular Messaging Data Collection Tool Online Help.

12. Verify the MSS trusted server passwords are populated.

13. Click Next.

14. On the MAS accounts and passwords screen:
   - a. Enter the correct logon name for each MAS administration account.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
b. Enter the password for each account. By design, the DCT tool does not automatically insert passwords.

c. Click **Next**.

15. On the Logon accounts and passwords screen:
   a. Enter the correct logon name and password for the technical support account and the customer administration account. The names and passwords must comply with the security standards.
   
b. Click **Next**.

16. On the MAS service account screen, verify that **Run MAS services using LocalSystem** is selected. Click **Next**.

17. On the TTS and announcements screen, click **Next**.

18. On the MM service selection screen:
   a. Verify that the correct services are selected for each server. The DCT updates this information with each MAS that it analyzes.
   
b. To activate the Web Subscriber Options (WSO) application on an MAS, click the appropriate column.
      You can activate Web Subscriber Options only once per voice mail domain.
   
c. Click **Next**.

19. On the **Switch Integration** screen, do not change the settings. Click **Next**.

20. After you have opened each DCT screen and cleared any red-flagged items, the **Cancel** button changes to a **Complete** button. After you have entered and verified all required data, click **Complete**. The system displays a **Save** window. Save the **.mmdct** data file to a storage device.

21. After you save the file, the Data Collection Tool window closes.

22. Remove the storage device from the server to prevent any damage to the data file.

23. Continue with **Busying out ports on each MAS** on page 159.
Busying out ports on each MAS

Modular Messaging system should not take any calls during the upgrade. To achieve this, busying out the ports on each MAS and on the switch before you start the upgrade. Otherwise, messages spool on the MAS, and delay the upgrade.

Busying out the ports on each server and on the switch before you upgrade that server.

To busying out the ports on each MAS:

1. The PBX administrator must use the procedures appropriate for this PBX to busying out the ports for the MAS being upgraded. Depending on the switch integration, the administrator might be able to temporarily reroute calls to other MASs. Otherwise, callers into the system might hear ring-no answer or a busy signal.

2. Switch the monitor to show the correct MAS. For more information, see Switching the monitor to show the correct server on page 149.

3. Unplug all modems to the Modular Messaging system. Otherwise, the system sends unnecessary alarms to the remote technical support group throughout the upgrade procedure.

4. Use the Port Monitor to disable ports on each MAS:
   a. Click Start > Programs > Avaya Modular Messaging > Port Monitor. The system opens the Port Monitor window.
   b. Select all ports in the list: Click on the first port, hold down the Shift key, and click on the last port.
   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.

5. Proceed with Checking the spool folder on each MAS on page 160.
Checking the spool folder on each MAS

Before you upgrade the MAS, verify that any spooled messages are delivered:

1. Switch the monitor to show the applicable MAS.
2. Open Windows Explorer.
3. Navigate to the folder C:\Program Files\Avaya Modular Messaging\Server\Spool
4. Verify that the Spool folder contains no message files.

⚠️ CAUTION:
If the folder contains spooled messages, wait for the system to deliver them, which can take awhile.
5. When the Spool folder is empty, you can proceed with upgrading the MASs.
Performing pre-upgrade tasks

Backing up each MAS

You must backup the data on each MAS in the system before you back up the MSS.

To back up all the data on the Modular Messaging system, first send backup data from each MAS to the MSS. The MAS information will be backed up along with the MSS system data on the DVD-RAM disks.

To back up the data on each MAS:

1. Switch the monitor to show the correct MAS. See Switching the monitor to show the correct server on page 149.

2. To view the scheduled backup program for this MAS, double-click the Scheduled Tasks icon on the desktop.

3. In the Scheduled Tasks window, run an attended backup on this MAS:

   a. Right-click the backup task that is already set up. This task is named MAS Backup on most systems, but might have a customer-specified name for upgrades. Select Run.

   The system backs up the data on this MAS to the MSS. The Status column shows Running. When the backup is complete, the Status column goes blank.

   b. To verify the success of the backup:

      1. Double-click the Monitor icon on the desktop.

      2. In the left pane, expand Event Viewer (Local), and then double-click Application.

      3. Refresh the window display periodically until you see the two 8009 ntbackup events.

When the events indicate a successful backup, continue with Step 4.

Note:

If the backup fails to run, verify the backup settings:

- Double-click the task MAS Backup to view the properties window.

- In the MAS Backup window, click the Task tab. Verify that the Run as field shows an account that has permissions to run manual backups, such as privdom\dom-admin. If the account is incorrect, enter the correct value.

- If you change the account, or to verify the password, click Set password. In the Set Password window, enter and confirm the password for the account. Click OK.

- Click OK to close the MAS Backup window.

- Run the backup again.

4. Close the Scheduled Tasks window.

5. Repeat steps 1 - 5 on each MAS in the system.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Upgrading to Modular Messaging Release 5.0 on S3500-family server

⚠️ CAUTION:  
If any MAS backup fails to complete, Do not proceed with the upgrade. Contact your remote support center for assistance.

---

### Backing up the MSS

After you back up each MAS to the MSS, you then back up all data from the MSS to the DVD:

1. Connect the console to the MSS by switching the KVM.
2. Log on to the MSS server as **craft**.
   - The system displays the Messaging Administration main menu.
3. Verify the number of subscribers:
   a. From the Messaging Administration menu, click **Subscriber Management**.
   b. Make a note of the number of subscribers.
4. Stop the messaging service:
   a. From the **Utilities** menu, click **Stop Messaging**.
   - The system opens the **Stop Messaging Software** page.
   b. Click **Stop**.
5. After the system reports that the voice system has completely stopped, begin an attended backup:
   a. From the **Backup/Restore** menu, click **Backup**.
   b. On the **Backup** page, set all data types to **Yes**.
   c. Verify that **Media Type** is set to **DVD-RAM**.
   d. Click **Save** or **Start Backup**.
   e. If the system opens an SSH Authorization window, log in as **craft**.
   f. The system warns you to not exit the backup page. Click **OK**
6. The system estimates the number of DVDs required. Verify that you have enough DVDs. Press **Enter** or click **Continue**.
7. Insert a labeled, writable DVD-RAM into the DVD drive. Press **Enter** or click **Continue**.
8. The system saves the new system configuration to the DVD. Allow about 30 minutes for each DVD.
9. Follow the prompts on the screen to track and complete the backup process. Scroll to the bottom of the page to see the most recent status messages. The message **FULL-MANUAL BACKUP completed successfully** indicates that the backup is complete.
Performing pre-upgrade tasks

⚠️ CAUTION:

If the attended backup does not complete successfully, **DO NOT** proceed with the upgrade. Contact your remote support center for assistance.

10. After the backup is complete, press the eject button on the front of the DVD-RAM drive, and remove the DVD-RAM backup medium. Change the tab on the DVD-RAM backup to write-protect.

11. Continue with [Running the Backup Verification tool on page 164](#).
Running the Backup Verification tool

The Backup Verification tool examines each disk and verifies if the system's data has a reliable backup. Use this tool after a preupgrade backup, before you proceed with an "irreversible" upgrade. To install the Backup Verification tool, see Installing the Pre-upgrade and Backup Verification tool on page 153.

Running the Backup Verification tool does not affect service. Run the Backup Verification tool on the day of the upgrade:

1. At the MSS prompt, log in as tsc, craft, or dadmin.
   The server displays the Messaging Administration main menu.

2. On the main menu, click Utilities > Backup/Restore > Backup Verification Tool.
   The Show Last Summary button only appears if someone has run the tool once before. Click the button if you want to view the previous summary information.

3. Insert the first DVD into the MSS.

4. On the Backup Verification Tool menu, click Start.

5. The system displays a warning if you verify a backup from a different Modular Messaging system. Click Yes to proceed or Abort to stop.
   Once the Backup Verification tool begins to run, the output displays the percentage of the verification that is complete and what file it is being verified.

6. If you use Netscape, the system might display the Netscape is unable to locate the server localhost error dialog box. This can happen for various reasons, such as if the verification takes longer than 15 minutes.
   If the system displays Netscape error dialog box:
   a. On the error dialog box, click OK.
   b. On your browser, click Reload.
      You must reload the page so that the output can continue to display the status of the backup verification.

7. If you abort the Backup Verification tool (by clicking Abort) for whatever reason, when you next try to run the tool do the following:
   a. On the Backup Verification Tool menu, click Stop Runaways if the button is available.
      Anytime you are starting the Backup Verification tool and the Stop Runaways button appears on the menu, click it.
   b. Click Start.
      When the verification is complete, a validation box appears.

8. Click OK.
   The system displays verification output.
9. Review the output for the current DVD:
   - A successful backup displays **Backup Verification Succeeded with no Errors.** If successful, proceed with step 10.
   - If the tool detects a bad backup the output log displays: **The Following Errors (or Warnings) Were Found in the Backup Set.** Return to the MSS main menu and redo the backup.

10. Repeat this procedure for every backup DVD.

11. After you verify that backup of every DVD is successful, return to the **Messaging Administration** main menu.
Upgrading the MSS from Release 3.x or Release 4.0

Perform the following and make sure you install software from both the OS and Application DVDs before you reboot the system:

1. Log on to the MSS as craft; see Logging on to the MSS on page 22.
2. Insert the Modular Messaging R5.0 MSS OS disk into the MSS.
3. From the Messaging Administration main menu, under Software Management, click Software Update > CD/DVD.
4. Click Install the newer software management software.
5. From the status page that appears, click Continue.
6. A warning page may appear saying that you have not backed up your system recently. If this page appears, do ONE of the following:
   - Click Continue without current system backup if you do not want to back up the system.
   - Click Cancel to stop the software update, at which time you can perform a system backup. After the backup is complete, repeat this process from the beginning.
7. On the page which lists the upgrade packages, click Install selected packages.
8. If a pop-up window appears, click Continue.
9. On the page which lists the upgrade packages, click Proceed with Installation.
10. On the status page that appears, scroll to the bottom of the page to see the most recent status messages.
11. After the system successfully installs the packages, remove the Modular Messaging R5.0 MSS OS disk.

⚠️ Important:
Do not reboot now; wait until you have finished with the MSS Application disk as explained below.

12. Insert the Modular Messaging R5.0 MSS Application disk into the MSS.
13. Click Update software from other media.
14. On the page that appears, click CD/DVD.
15. A warning page may appear saying that you have not backed up your system recently. If this page appears, do one of the following:
   - Click Continue without current system backup if you do not want to back up the system.
   - Click Cancel to stop the software update, at which time you can perform a system backup. After the backup is complete, repeat this process from the beginning.
16. On the page that appears, which lists the upgrade packages, click **Install selected packages**.

17. If a pop-up window appears, click **Continue**.

18. On the page that appears, which lists the upgrade packages, click **Proceed with update**.

19. On the status page that appears, scroll to the bottom of the page to see the most recent status messages.

20. After the system successfully installs the packages, remove the Modular Messaging R5.0 MSS Application DVD, and then click **Reboot**.

**Note:**

After this update, when you log into the console browser you might see a message about Firefox updates; if the message appears, click **Cancel**.
Upgrading an MAS from Release 3.x or Release 4.0

Upgrading an MAS from Release 3.x or Release 4.0 to Release 5.0 involves performing the following procedures on each MAS; complete the processes on one before you proceed to the next MAS:

- Logging off all remote logins on page 168
- Upgrading overnight on page 168
- Upgrading RealSpeak on page 168
- Upgrading Dialogic drivers on page 171
- Upgrading the MAS software on page 172

After you complete the upgrade for each MAS, proceed with the procedures in Completing the upgrade from Release 3.x or Release 4.0 on page 176 to complete the upgrade process.

Logging off all remote logins

Use these steps to log off all remote logins:

1. Bring up your Task Manager and select the Users tab.
2. Select remote logins and click Logoff.

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, enable the tasks again. After you complete the upgrade successfully, you must enable the scheduled tasks again when you perform the procedures in Completing the upgrade from Release 3.x or Release 4.0 on page 176.

If you upgrade from Release 4.0, proceed with instructions outlined in Upgrading Dialogic drivers on page 171.

Upgrading RealSpeak

Complete the following tasks only if you are upgrading from Release 3.x.

- Stopping all MM services on page 169
- Uninstalling and re-installing RealSpeak on page 169
Starting all MM services on page 171

Stopping all MM services

You need to stop all MM services on each MAS that you upgrade. Perform these steps only if you are upgrading from a Release 3.x system:

1. Make a list of all MM Services running on this MAS, you'll need this list later.
2. Switch the monitor to show the correct MAS.
3. 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 Intel Dialogic services and some Windows services.

4. Confirm that all Modular Messaging services are stopped:
   a. Double-click the Monitor icon on the desktop or from the command prompt, run services.msc.
   b. Click Services (Local) in the left pane, if the item is not already selected.
   c. If the Monitor window was already open, refresh the screen.
   d. In the right pane, scroll down to the list of installed Modular Messaging services. These all start with the abbreviation MM.
   e. Verify that the Status column is blank. If any service is not stopped, repeat Steps 3 and 4.

Uninstalling and re-installing RealSpeak

Perform these steps only if you are upgrading from a Release 3.x system:

You must complete the following when performing an upgrade:

1. Log onto the MAS using the Windows Account used to install the original RealSpeak.
   For MAS#1 this will be the domain administrator account, and for subsequent MASs this is the local administrator account.

2. Insert the Modular Messaging R5.0 MAS Application DVD 2 of 2 disk into the MAS.

3. From the DVD, run the RealSpeakUninstallRealspeak.bat file.

4. The MAS should automatically reboot; if it does not, manually reboot the MAS.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
5. Log back onto the MAS using the Windows Account used in Step 1.
6. On the MAS, delete the folder: C:\Program Files\ScanSoft.
7. From the Modular Messaging R5.0 MAS Application DVD 2 of 2 disk, run the RealSpeak\installRSEngine.bat file.
8. On the InstallShield Wizard, click Next.
9. Select I accept the terms in the license agreement and click Next.
10. On Custom Setup, keep the default settings and click Next.
11. On RealSpeak Host service, keep the default setting and click Next.
12. On Ready to Install the Program, click Install.
   A window shows the installation status.
13. When the installation is complete, click Finish.
14. On the pop-up window, click Yes to restart the system.
15. Log back onto the MAS using the customer account.
16. In the Modular Messaging R5.0 MAS Application DVD 2 of 2 disk, locate and launch the RealSpeak\installRSLangs.bat file to install RealSpeak languages.
   The system displays the status of each language installation.
17. Remove the Modular Messaging R5.0 MAS Application DVD 2 of 2 disk.
Starting all MM services

Restart the MM services and verify that the services are running. Perform these steps only if you are upgrading from a Release 3.x system:

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 Modular Messaging services correctly.
3. Verify that the Modular Messaging services are set correctly.

Upgrading Dialogic drivers

Complete this procedure for upgrades from Release 3.x and Release 4.0.

If the MASs use Dialogic port boards or if the MASs have the Dialogic driver installed, complete the following.

1. Log onto the MAS using the customer account.
2. Insert the Modular Messaging R5.0 MAS Application DVD 1 of 2 into the MAS.
3. Uninstall Dialogic drivers:
   a. From the DVD, run the **Dialogic_Drivers\MMDialogicUnInstall.bat** file.
   b. On the Question window that prompts for a backup, click **No**.
   c. On the Confirm Uninstall window, click **OK**.
      
      A window appears that displays the uninstall status.
   d. On the Maintenance Complete window, select **Yes, I want to restart my computer now** and then click **Finish**.
4. Log onto the MAS using the customer account.
   The system runs the **Clean-up Utility** automatically.
5. On the Hardware Update Wizard, click **Cancel**.
6. Reinstall Dialogic drivers:
   a. From the DVD, run the **Dialogic_Drivers\MMDialogicUpgrade.bat** file.
   b. On the Dialogic(R) System Release window, click **Next**.
   c. On the Customer Information window, keep the default names and click **Next**.
   d. On the Choose Destination Location window, keep the default location and click **Next**.
   e. On the **Select Features** window, keep the default selection(s) and click **Next**.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Upgrading to Modular Messaging Release 5.0 on S3500-family server

f. On the Question window, click Yes.
g. If a warning window about Java appears, click OK.
h. On the Select Program Folder window, keep the default folder and click Next.
i. On the Start Copying Files window, click Next.
   The Setup Status window displays the installation status. After the Dialogic files install, a
   Found New Hardware window appears.
j. Select No, not this time, and click Next.
k. Select Install the software automatically, and click Next.
l. If an unsigned driver dialog box appears, click Yes.
m. After the board is set up, click Finish.
n. Repeat this for all Dialogic boards installed on this MAS.
o. On the Setup Complete window, select to restart your computer at this time and click
   Finish.

7. Log on to the MAS using the customer account.

8. From the DVD, run the Dialogic_Drivers\mm_install\SetDialogicSettings.exe file. This
   restores the Dialogic configuration for your MAS.

9. Start the Dialogic drivers:
   a. Click Start > Programs > Intel Dialogic System Release > Configuration Manager -
      DCM.
   b. The Intel Dialogic product Configuration Manager window opens.
   c. From the Intel Dialogic product Configuration Manager window, on the button bar, click
      the green > (Start) button.
   d. Wait for the devices to start and the installed boards to show a green light.
   e. Close the DCM window.

Upgrading the MAS software

The following steps explain how to upgrade the MAS software.

   Note:
       Remote Desktop updates are not supported.

It is important to perform the tasks in the following order:
1. Log onto the MAS using the customer account.
2. Verify that MM Service Connector is set to Automatic.
3. Ensure that all Windows applications are closed.
Upgrading an MAS from Release 3.x or Release 4.0

4. Close all monitoring tools, such as the port monitor.

5. Insert the ‘Avaya Modular Messaging R5.0 MAS Application DVD 1 of 2’ disk.

6. From the DVD, run **Install\setup.exe** and complete the following:
   a. Verify that Select Configuration lists **Avaya MSS**.
   b. Make sure that you select the **Enable Windows Installer logging** check box in the lower left-hand corner. Select the check box if it is not already selected.
   c. Make sure that you select the **MM Configuration Tools** checkbox.
   d. Expand the prompts and select any prompts that are not already selected.
   e. Click **Install**.
   f. On the **System Upgrade** window, click **Run System Upgrade**.
   g. When the system prompts you, on the **Installation Wizard** window, click **Restart**. The system restarts.
   h. Log on using the customer account.
   i. If any patches exists on the system:
      1. The system displays a window that displays the patches to be uninstalled. Follow the prompts.
      2. Patch uninstaller may require server restarts. If the system prompts you, restart the server.
      3. If the server restarts, the MM Installation wizard automatically launches. If it does not, then manually run **Install\setup.exe**.
   j. Return to Step a to verify the configuration settings.
      The system upgrades the Modular Messaging software components. As the components window shows which component is installing it will pause on Avaya SPIRIT Agent for several minutes. This is an expected behavior.
   k. Restart the server when prompted.

7. When the server starts, log in to the server using the customer account.
   The MM Configuration Wizard runs automatically, displaying the Service configuration window.

8. Follow the installation Configuration Wizard prompts.

9. When complete, click **Finish**.

10. Verify that all the appropriate Modular Messaging services are enabled on an MAS. For the list of services that are to be enabled on each MAS, see **Enabling Modular Messaging services in a VMD** on page 78.

11. Install the latest Avaya Service Pack (SP). For more information, see **Installing software updates** on page 175. The patch install notes will be in the patch distribution folder along with the patch. The system restarts Modular Messaging services automatically.

**Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.**
12. You **must** obtain a new RFA license for your upgraded system, which includes setting up 12 TTS sessions per MAS. For instructions, see *Getting and installing a license on MAS#1* on page 63.

13. Perform the following steps if you are upgrading from Release 3.x.
   
   a. Enter the product ID for the current MAS; see *Entering Product ID for current MAS* on page 65.

   b. 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. For additional information, see *Configuring serviceability settings on MAS#1* on page 61.

   c. Configure the MM Audit Service; see *Configuring MM Audit Service* on page 69.

   d. Configure the MM Fax Service:

   - Run `C:\Avaya_Support\Utils\FaxSenderEnable.exe` on the machine that hosts the MM Fax Sender service.

   - Restart the Microsoft Fax Service.

   - Complete all of the steps in *Configuring the MM Fax Sender service* on page 70.

14. Do the following as appropriate:

   a. If you have additional MASs or Supplementary server to upgrade, continue with *Upgrading an MAS from Release 3.x or Release 4.0* on page 168.

   b. Proceed with *Completing the upgrade* on page 176.
Installing software updates

The Modular Messaging Release 5.0 software is the most current version available at the time of release. However, you need to update the software after an upgrade to include the latest changes. Avaya provides these updates in the form of an Avaya Service Pack (SP) or a software patch.

Complete the following steps to update Modular Messaging software:


   Note:
   If you followed the procedure for Downloading software updates on page 10, you already downloaded any required software updates.

2. Follow the instructions provided in Updating Modular Messaging software on page 323 to update the system with the latest changes before you do acceptance testing.
Completing the upgrade from Release 3.x or Release 4.0

This section describes the topics required to complete the upgrade of Modular Messaging system to Release 5.0.

Completing the upgrade

Note:
You do not need to upgrade the offline access (OLA) server, as the server does not run any Modular Messaging services.

After you complete the upgrade of all MASs and the Supplementary server, if present (Upgrading an MAS from Release 3.x or Release 4.0 on page 168), perform the following procedures:

1. If you upgraded overnight, use the Voice Mail System Configuration application to enable the tracing database nightly tasks.
2. Do the acceptance tests that are appropriate for each server; see Performing acceptance tests for a new installation on page 111. 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.
3. Run a DCT analyze on the system; see Using the DCT to analyze the current configuration on page 136.
4. Back up the DCT data files; see Copying the DCT data file for backup on page 132.
5. 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.
Completing the upgrade from Release 3.x or Release 4.0

   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 any discrepancies in the schedule grid.

   f. Close all windows.

6. Review event and alarm logs and resolve any problems; obtain the Avaya Modular Messaging MAS Administration Guide; see Downloading user documentation on page 12.

7. Run backups on each MAS; see Backing up each MAS on page 161. You DO NOT need to remove the old backup files from the MSS.

8. Run a backup on the MSS; see Backing up the MSS on page 162. If using DVD-RAM, use a separate DVD-RAM disk to avoid overwriting the backup data from the previous release that is saved during the pre-upgrade steps.

9. Perform this step only if you are upgrading from Release 3.x. Due to a change in file names, older logs might remain on the system. Remove older logs from c:\avaya_support\logs folder on each MAS and delete any logs that are older than the upgrade’s start time.

10. On the Messaging Administration web interface, complete the following:

    a. Under the Alarming menu, click Alarming Configuration.

       The system opens Configure Alarms page.

    b. In the Alarm Suppression field, click INACTIVE.

11. On the MAS, enable 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, clear Suppress alarm notifications check box, to turn on the alarm notifications options.

    d. Click Save to save the changes.

    e. Close all windows.

This completes the upgrade of Modular Messaging system to Release 5.0.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
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 servers, which have been upgraded to Modular Messaging Release 5.0.

1. Run the registry file, C:\Avaya_Support\Registry_Keys\convertsupp_2_0portmas.reg.

2. Under the Messaging Administration of the Messaging Administration web interface, click Trusted Servers. The system displays Manage Trusted Servers page. Do one of the following:
   - Change the trusted server for the Supplementary server using the following steps:
     a. Highlight the Trusted Server with a service name of Supplementary Server. Click Edit the Selected Trusted Server.
     The server displays the Edit Trusted Server page.
     b. In the Special Type field, click Messaging Application Server from the drop-down list.
     c. Click Save.
   - Create the trusted server for the Supplementary server using the following steps:
     a. Click Add a New Trusted Server.
     The server displays the Add Trusted Server page.
     b. In the Special Type field, click Messaging Application Server from the drop-down list.
     c. Click Save.

3. Install MMFEDB.
   a. Copy all the contents from <cd drive>\Install\System Upgrade\SQL2005EXP of the 'Avaya Modular Messaging R5.0 MAS Application DVD 1 of 2' disk to the C:\MM_SYSTEM_UPGRADE directory of the MAS.
   b. If the system prompts you, select to overwrite all existing files.
   c. Double-click the C:\MM_SYSTEM_UPGRADE\setup.bat file.
   d. Click Option 1 to install MMFEDB.
Converting Supplementary server to run a 0 port MAS on the Supplementary server

e. Wait for MMFEDB install to complete.
   Installation process takes some time. The system opens and closes various windows
   installation dialogs boxes automatically. Do not make any manual intervention.

4. Set the MM MAS service to **Automatic**. Do not start the service at this time.

5. Ensure that the MM Service Connector service is set to **Automatic**. Do not start the service
   at this time.

6. Ensure that the MM Fault Monitor service is set to **Automatic**. Do not start the service at
   this time.

7. Ensure 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.

8. Locate and run **gvconfig.exe**:
   a. Locate and run \C:\Program Files\Avaya Modular Messaging\VServer\Config\gvconfig.exe
   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 R5.0 MAS Application DVD 1 of 2’ disk in to the Supplementary server DVD
      drive.
   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.

**Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.**
Upgrading to Modular Messaging Release 5.0 on S3500-family server

9. Configure MAS Host Setup on the Supplementary server.
   a. On the Messaging Administration web interface, click **Server Administration > MAS Host Setup**.
      The system opens **Setup MAS Host Information** page.
   b. In the **MAS ID** field, click the appropriate MAS for the supplementary server.
      Use the lowest available MAS. For example, if you have two MASs and one Supplementary server, then add the Supplementary server as MAS Host Setup for MAS3.

10. Send the MAS host information to all MASs.
   a. On the Messaging Administration web interface, click **Server Administration > MAS Host Send**.
      The system opens **Send MAS Host Information** page.
   b. Click **Send**.
      The system sends the host information to all MASs at the same time and reports whether the information was updated successfully. For more information, see Updating MAS host information on page 103.

11. Double-click the **C:\Avaya_Support\Tools\ServiceControl\StopMMServices.exe** file to stop all MM services.

12. 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 181
- **Changing from DSE or QSIG to H.323** on page 183
- **Changing from DSE or QSIG to SIP** on page 184
- **Changing from QSIG T1 to QSIG E1** on page 185
- **Changing from H.323 to SIP** on page 187

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 5.0 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 to Manual that are running on the MAS:
   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. Shutdown the MAS.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
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. Shutdown 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 277.

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 Modular Messaging services on page 239.

14. Test the QSIG integration; see Verifying call-handling capability on page 80.

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 156.
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 5.0 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 to Manual that are running on the MAS:
   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 for board removal and installation.

6. Start the MAS.

7. 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.

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 Modular Messaging services on page 239.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
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 80.

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 156.

**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 156.

   You will not be changing the Switch Integration type at this time.

2. Upgrade all MASs in the Voice Mail Domain (VMD) to Release 5.0 as explained in this chapter.

3. After completing the upgrade, use the VMSC to apply your new Modular Messaging Release 5.0 license, which will include the SIP certificate; see Obtaining and installing a license on MAS#1 on page 60.

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](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 Modular Messaging services on page 239.

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 80.

9. Shutdown 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 and installation.

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 156.

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 5.0 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 to Manual that are running on the MAS:
   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. See Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions guide.
9. Start the MAS.
10. Configure the boards using DCM; see Configuring port boards on page 277.
11. Start the MAS service:
   a. Once 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 Modular Messaging services on page 239.

14. Test the QSIG integration; see Verifying call-handling capability on page 80.

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 156.
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 5.0 as explained in this chapter.

2. After completing the upgrade, use the VMSC to apply your new Modular Messaging Release 5.0 license, which will include the SIP certificate; see Obtaining and installing a license on MAS#1 on page 60.

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 Modular Messaging services on page 239.

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 80.

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 156.
Moving to the corporate Windows domain after upgrade

⚠️ Important:
If the system will remain in the private Windows domain, you can skip this entire section.

After you upgrade to Release 5.0, you can move the Avaya Modular Messaging system to the customer’s corporate Windows domain. This feature is optional and is beneficial to those customers who do not want a separate private Windows domain within their network.

Perform the following tasks to move a system during an upgrade to the customer’s corporate Windows domain:

- [Preparing to join an upgrade to the corporate Windows domain](#) on page 189.
- [Moving subsequent servers to the corporate Windows domain](#) on page 190.
- [Moving the MSS to the corporate Windows domain](#) on page 194.
- [Moving MAS#1 to the corporate Windows domain](#) on page 194.
- [Completing the move to the corporate Windows domain](#) on page 196.
Preparing to join an upgrade to the corporate Windows domain

The following explains how to prepare an MM system that is joining the corporate Windows domain after an upgrade:

1. Complete the upgrade to Release 5.0, as described in this chapter.
2. Create user accounts in the corporate Windows domain; see Creating user accounts in the corporate Windows domain on page 17.
3. Create computer accounts in the corporate Windows domain; see Creating computer accounts in the corporate Windows domain on page 18.
4. Update the DNS. If the customer is going to use a different DNS server, update the corporate LAN DNS settings for each MAS and the MSS. This step MAY NOT be necessary as the existing DNS configuration may be correct. Make sure that the Corporate Domain Name can be resolved with this configuration or joining the MM system to the corporate Windows domain will fail. Complete the following:
   a. Change the DNS settings for the MSS; see Setting up network addressing on page 27.
5. Continue with Moving subsequent servers to the corporate Windows domain on page 190
Moving subsequent servers to the corporate Windows domain

When moving your MM system to the corporate Windows domain, you must first move all subsequent MASs (MAS#2 and above) and, if present, the Supplementary server and optional servers BEFORE you move the MSS or MAS#1.

⚠️ Important:
DO NOT MOVE the MSS or the MAS#1 at this time. These servers are covered later in this section.

Preparing the system before moving subsequent servers

To prepare the system before moving subsequent servers (MAS#2 and above) to the Corporate Windows Domain:

1. Verify that logon accounts in the corporate Windows domain were created during the pre-installation stage; see Creating user accounts in the corporate Windows domain on page 17.

2. Be sure that you have the local administrative account and password for all MASs and, if present, the Supplementary server and optional servers. To be sure, log into each server to verify.

   Determine if the customer’s corporate Windows domain has a policy established to change the local administrative account and password when new machines move to the corporate Windows domain. If this is the case, then make sure you have the local administrative account name and password that will be assigned after all MASs move to the corporate Windows domain.

3. Click Start > Run.

4. In the Run window Open field, type cmd and press Enter.

5. In the command prompt window, type the following and press Enter:
   
   net time /setsntp

6. Run a DCT analyze on the system; see Using the DCT to analyze the current configuration on page 136.

7. Back up the DCT data files; see Copying the DCT data file for backup on page 132.

8. Manually run a backup of all MASs and, if present, the Supplementary server and optional servers; see Backing up each MAS on page 161.
9. Run a backup of the MSS; see Backing up the MSS on page 162.

⚠️ Important:
Make sure you complete steps 1 through 9 before continuing.

10. Disable the Offline Access feature. Otherwise, errors occur as the system searches for the missing offline store.
   a. For MAS#1, in the Voice Mail System Configuration window, double-click **Messaging**.
   b. In the Messaging - Voice Mail Domain window, click the **Offline Access** tab.
   c. Clear the checkbox to **Enable offline access to messages**. Click **OK**.
   d. After all servers in the system are upgraded, re-enable Offline Access feature:
      1. In the VMSC window, double-click **Messaging**, and then click the **Offline Access** tab.
      2. Click the checkbox to **Enable offline access to messages**.
      3. Click the checkbox to **Synchronize offline messages with remote store**.
      4. Click **Browse** to select an existing, shared folder in the domain for the remote offline message store. The name **must** use the format `\computername.privdom.local\sharename`, such as `\mymas2.privdom.local\RemoteOfflineStore`.
      5. Click **OK** to close this window.

⚠️ Important:
The following step is extremely important. All access to the VMD will be lost if this step is not completed.

11. Using VMSC, add **Everyone** to the VMD System Administration ACL using the following steps:
   6. In the Permissions window, click **Add**.
   7. In the Select Users, Computers, or Groups window, type the first letter of the account to add in the **Enter the object names to select** box.
      For example, type **e** for **Everyone**.
   8. Click **Check Names**.
   9. In the Multiple Names Found window, double-click the correct account.
   10. Verify that the account is listed and underlined in the list box.
   11. Click **OK**.
   12. **Optional**: Repeat this task to add other logon accounts, if required.
   13. Give the correct share permissions to the accounts. In the Permissions window:
      - Select each account in turn.
      - In the **Permissions** box, under **Allow**, select the permissions **Change** and **Read**, so the boxes are checked.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Upgrading to Modular Messaging Release 5.0 on S3500-family server

- Repeat this task for each logon account.

12. Click OK to close the Permissions window.

Moving subsequent servers

⚠️ Important:
Complete Preparing the system before moving subsequent servers on page 190 before continuing.

To move subsequent servers (MAS#2 and above) and Supplementary servers to the corporate Windows domain:

1. Log into the MAS using the private domain administrator account.

2. Stop all MM Services on the server you are moving to the corporate Windows domain; see Starting all MM services on page 171.

3. Set the MM Services that are not disabled 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. Delete the lmhosts file found in:
   C:\Windows\system32\drivers\etc\

5. Move the MAS directly from the private Windows domain to the corporate Windows domain:
   a. Right-click My Computer and click Properties.
   b. Click the Computer Name tab.
   c. Click Change.
   d. In the Member of box, select Workgroup and type WORKGROUP into the provided field.
   e. Click OK and then select to restart the computer.
   f. After the restart, log back on as the local administrator account.
   g. If necessary, reconfigure the Corporate LAN settings.
   h. Right-click My Computer and click Properties.
i. Click the **Computer Name** tab.

j. Click **Change**.

k. In the Member of box, select **Domain** and type the corporate Windows domain name into the provided field.

l. Click **OK** and then select to restart the computer.

6. After the restart, log back on as the local administrator account.

7. Add the corporate Windows domain customer account and technical support account to the local machine’s Administrators group:

   a. Right-click **My Computer** and click **Manage**.

   b. Click **Local Users and Groups**.

   c. Double-click **Groups**.

   d. Double-click **Administrators**.

   e. Click **Add**.

   f. Change **From this Location** to point to the corporate Windows domain.

   g. In the Enter the object names to select field, enter the name of the corporate Windows domain customer account (or technical support account) and click **Check Names**.

   h. Highlight the customer account (or technical support account) from the list of accounts resolved.

   i. Click **OK**.

   j. Repeat steps e through i as needed to add both the technical support account and the customer administration account to the local machine’s Administrators group.

8. Log off the server.

9. Log on to the server and the corporate Windows domain using the corporate Windows domain customer account.

10. Start all MM services that were previously running on this MAS and set them to automatic startup; see **Starting all MM services** on page 171.

11. Repeat these steps for all subsequent MASs and, if present, the Supplementary server and optional servers.

12. When MAS#1 is the only server left in the private Windows domain, continue with **Moving the MSS to the corporate Windows domain** on page 194.

**Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.**
Moving the MSS to the corporate Windows domain

To move the MSS to the corporate Windows domain:

1. Update the MAS host information; see Upgrading MAS host information in a corporate Windows domain on page 100.
2. Place the MSS in the corporate Windows domain; see Placing the MSS in the corporate Windows domain on page 103.

Moving MAS#1 to the corporate Windows domain

To move MAS#1 to the corporate Windows domain:

1. Stop all MM Services on MAS#1; see Starting all MM services on page 171.
2. Set the MM Services that are not disabled 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.
3. Delete the lmhosts file found in:
   C:\Windows\system32\drivers\etc\ 
4. Run the setsntp command:
   a. Click Start > Run.
   b. In the Run window Open field, type cmd and press Enter.
   c. In the command prompt window, type the following and press Enter:
      net time /setsntp
5. Run DCPromo to demote MAS#1 from being the Domain Controller for the private Windows domain:
   a. On MAS#1, click Start > Run...
   b. In the Run dialog box, type dcpromo, then click OK.
c. Click **Next**.
d. In the Warning dialog box, click **OK**.
e. Click the checkbox: **This server is the last Domain Controller in the Domain**.
f. Click **Next**.
g. Click **Next**.
h. Click the checkbox: Delete all application partitions on this DC.
i. Click **Next**.
j. Enter and confirm the Local Administrator password.
k. Restart MAS#1.
l. Click **Next**.
m. Click **Next**.
n. Click **Finish**.
o. Click Restart Now.

6. Log on to MAS#1 using the local administrative account.

7. Move MAS#1 to the corporate Windows domain:
   a. Right-click **My Computer** and click **Properties**.
   b. Click the **Computer Name** tab.
   c. Click **Change**.
   d. In the Domain name field, replace the existing private Windows domain name with the corporate Windows domain name.
   e. Click **OK**.
   f. Click **OK**.
   g. Restart the server.

8. Log on to MAS#1 using the local administrative account.

9. Add the corporate Windows domain customer account and technical support account to the MAS#1 Administrators group:
   a. Right-click **My Computer** and click **Manage**.
   b. Click **Local Users and Groups**.
   c. Double-click **Groups**.
   d. Double-click **Administrators**.
   e. Click **Add**.
   f. Change **From this Location** to point to the corporate Windows domain.
Upgrading to Modular Messaging Release 5.0 on S3500-family server

- In the Enter the object names to select field, enter the name of the corporate Windows domain customer account (or technical support account) and click **Check Names**.
- Highlight the customer account (or technical support account) from the list of accounts resolved.
- Click **OK**.
- Repeat steps e through i as needed to add both the technical support account and the customer administration account to the MAS#1 Administrators group.
- Go back to **Local Users and Groups**.
- If necessary, rename the local administrator account name from Administrator to the name that appears on the planning form.

10. Log off MAS#1.
11. Log on to MAS#1 and the corporate Windows domain using the corporate Windows domain customer account.
12. Start all MM services that were previously running on this MAS and set them to automatic startup; see **Starting all MM services** on page 171.

Completing the move to the corporate Windows domain

To complete the move to the corporate Windows domain during an upgrade you must reset the MM System shares, the backup tasks, and the time server configuration:

1. Recreate the Offline Store share and add computer$ accounts for all MASs in your VMD on the server that hosts the Offline Store feature:
   - Using Windows Explorer locate the **Remote Offline Store** folder.
   - Right-click the folder name and click **Properties**.
   - Click the **Sharing** tab.
   - Click **Share this folder**.
   - Click **Permissions**.
   - Under Groups and Users, click **Add**.
   - Add **Computers** into the list of Object Types.
   - In the Object name window, enter the corporate domain name of the MAS.
   - Click **Check Names**.
   - Highlight the name of the MAS and click **OK**.
   - Set the permissions for the MAS local machine account to **Allow Change and Read**.
   - Repeat steps g to k for all MASs that handle calls.
2. Change the mini backup batch file so that it contains the corporate Windows domain name for the MSS:
   a. Locate file: `C:\Avaya_Support\CMD\MASminiBackup.bat`
   b. Open the file so that you can edit its content.
   c. Change the line:
      ```
      net use v: \mss1\masbackup
      ```
      to
      ```
      net use v: \msscorporatename\masbackup
      ```
      where `msscorporatename` is the corporate Windows domain name of the MSS.
   d. Save and close the file.
3. Change backup batch file so that it contains the corporate Windows domain name for the MSS:
   a. Locate file: `C:\Avaya_Support\CMD\MASBackup.bat`
   b. Open the file so that you can edit its content.
   c. Change the line:
      ```
      net use v: \mss1\masbackup
      ```
      to
      ```
      net use v: \msscorporatename\masbackup
      ```
      where `msscorporatename` is the corporate Windows domain name of the MSS.
   d. Save and close the file.
4. Change the DCT Analyze scheduled tasks so that they run under the new corporate Windows domain customer account:
   a. Double-click the **Schedule Tasks** icon on the desktop.
   b. In the list of Scheduled Tasks, open the DCT Analyze properties.
   c. Click the **Task** tab.
   d. Change the **Run as** entry to be the corporate Windows domain customer account.
   e. Click **Set Password**.
   f. Enter and confirm the corporate Windows domain customer account password.
   g. Click **OK**.
   h. Click the **Security** tab.
      i. In the Group or User Names window, remove the Private Domain Administrators Group.
      j. Add the corporate Windows domain customer account to the security list.
Upgrading to Modular Messaging Release 5.0 on S3500-family server

k. Change the permissions for the corporate Windows domain customer account to Full Control.

5. Change the scheduled tasks Nightly backup so they run under the new corporate customer account:
   a. Double-click the Schedule Tasks icon on the desktop.
   b. In the list of Scheduled Tasks, open the MAS Backup properties.
   c. Click the Task tab.
   d. Change the Run as entry to be the corporate Windows domain customer account.
   e. Click Set Password.
   f. Enter and confirm the corporate Windows domain customer account password.
   g. Click OK.
   h. Click the Security tab.
   i. In the Group or User Names window, remove the Private Domain Administrators Group.
   j. Add the corporate Windows domain customer account to the security list.
   k. Change the permissions for the corporate Windows domain customer account to Full Control.

6. Change security settings in VMSC for all accounts (corporate customer and technical support accounts, as well as all MAS computer accounts):
   a. Click Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration to open the VMSC window.
   c. Double-click System Administration.
   d. In the Permissions for System Administration window, click Add.
   e. In the Select Users, Computers, or Groups window, type the first letter of the account to add in the Enter the object names to select box.
   f. Click Check Names.
   g. In the Multiple Names Found window, double-click the correct account.
   h. Verify that the account is listed underlined in the list box, and then click OK.
   i. Perform steps a through h for all accounts:
      ● Corporate customer account
      ● Corporate technical support account
      ● All MAS computer accounts.
j. Select each **Account Unknown** entry, and then click **Remove**.

k. Select the **Everyone** account, and then click **Remove**.

l. Click **OK** to close the permissions window.

m. Return to Security and then double-click **Subscriber Administration**.

n. Add the corporate customer and technical support accounts, as well as all MAS computer accounts.

o. Remove all **Account Unknown** entries and also remove the **Everyone** account. Update the MAS host information on the MAS.

7. Run a DCT analyze on the system; see *Using the DCT to analyze the current configuration* on page 136.

8. Back up the DCT data files; see *Copying the DCT data file for backup* on page 132.
Upgrading to Modular Messaging Release 5.0 on S3500-family server
Chapter 9: Migrating to Modular Messaging Release 5.0 on S8730-family server

The chapter describes how to migrate from Release 2.0, Release 3.x or Release 4.0 to Modular Messaging Release 5.0 system that runs on S8730-family server. You can use this procedure to migrate from S3400 or S3500 to S8730.

Note:
You cannot upgrade from Release 2.0 to Release 5.0 or from S3400 server to S8730 server. Migration is the only way you can move the Modular Messaging system from:
- Release 2.0 to Release 5.0
- S3400 server to S8730 server

If you are upgrading to Release 5.0, and still use the S3500 server, use the procedures described in Upgrading to Modular Messaging Release 5.0 on S3500-family server on page 145.

If you are performing a staged upgrade, see Avaya Modular Messaging Staged Upgrades for the Avaya Message Store Server (MSS) Release 5.0 guide.

If you are moving the Modular Messaging system to the corporate Windows domain, first complete the entire migration and then move the system to the corporate Windows domain. See Moving to the corporate Windows domain after migration on page 252 for more information.

You may change the switch integration after you complete the process of migration. See Changing switch integration on page 251 for more information.

Topics in this chapter include:
- Migration requirements on page 202
- Preparing for the migration on page 204
- Migrating MSS and MAS to the S8730-family server on page 210
- Migrating each MAS on page 217
- Completing MSS administration on page 231
- Restoring data on each MAS on page 234
- Completing the system migration on page 242
- Reducing servers by replacing S3400 servers with S8730 servers on page 249
- Changing switch integration on page 251
- Moving to the corporate Windows domain after migration on page 252.
Migrating to Modular Messaging Release 5.0 on S8730-family server

Migration requirements

To successfully migrate a Modular Messaging system, you need:

- The original DCT file for the system or planning forms for the system that runs on Release 3.x.
- The latest analyzed DCT file for the 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 9.
  - The most current copy of the configuration notes for this switch integration.
  - The Avaya Modular Messaging MSS Pre-upgrade and Backup Verification Tool. For more information, see Installing the Pre-upgrade and Backup Verification tool on page 205.
  - Any Avaya software updates 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.
- Print the migration checklist from Modular Messaging Release 5.0 system migration checklist on page 269. Use the checklist to track your progress.
- When migrating from Release 2.0, all account names and passwords must conform to Windows 2003 R2 security rules. If they do not conform to the new rules, you must change account names and passwords 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.
Switching the monitor to show the correct server

You must switch the display from one server to another during a system migration. The Modular Messaging system might use a Belkin KVM switch or a customer-provided KVM switch. See Switching the monitor to show the correct server on page 149 for more information.
Preparing for the migration

This section describes how to prepare the Modular Messaging system that runs on S3400 or S3500 server while you migrate to Modular Messaging Release 5.0, that runs on Avaya S8730 server.

Avaya S8730 servers are supplied with MSS and MAS software pre-loaded on them.

When migrating from S3400 hardware, you may reduce the number of MASs in your VMD. For complete procedures to reduce MASs, see Reducing servers by replacing S3400 servers with S8730 servers on page 249.

Note:
The Modular Messaging Release 4.0 system must be at least at SP 3 and RFU level must be at least M8017rf+g, A6016rf+f, Z8017rf+c, E6016rf+b or U8017rf+b before you do the backup that will be used in the migration to Release 5.0 on an S8730 server.

Perform the following tasks to prepare the Modular Messaging system for the migration:

- Performing pre-upgrade tasks on page 205
- Using the DCT to collect information from an MAS on page 206.
Preparing for the migration

Performing pre-upgrade tasks

Perform the following tasks before you migrate the system:

- Installing the Pre-upgrade and Backup Verification tool on page 205
- Running the Pre-upgrade tool on page 205
- Completing pre-upgrade tasks on page 206

Installing the Pre-upgrade and Backup Verification tool

Install the MSS Pre-upgrade and Backup Verification Tool as outlined in Installing the Pre-upgrade and Backup Verification tool on page 153.

Running the Pre-upgrade tool

A member of the Avaya or business partner installation team uses the Pre-upgrade tool to identify potential pitfalls and plan for the migration. Run the Pre-upgrade tool using the steps outlined in Running the Pre-upgrade tool on page 153.
Completing pre-upgrade tasks

Complete the tasks outlined in Completing pre-upgrade tasks on page 155, before you start migrating to Release 5.0.

Adding a new server

If you are adding a new MAS to an existing Modular Messaging system, first migrate the system. After the migration is complete, install the new MAS. Adding an MAS or a Supplementary server to an existing system on page 341.

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. The tool puts the server system information into a data file. This allows you to easily configure the servers.

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 the latest version rather than the one on the applications DVD.

Collecting DCT data

Run a DCT analyze on each MAS and Supplementary server to collect system data as instructed in Using the DCT to analyze the current configuration on page 136.
Verifying DCT data

After analyzing the last MAS to be migrated, the Avaya Modular Messaging Data Collection Tool (DCT) window displays the results of the last analysis. The DCT collects most of the information that the system requires to migrate an MAS to Release 5.0. However, you must enter some data manually, and verify the information as described in this section.

For more information about completing the DCT screens, click the Help button in the Avaya Modular Messaging Data Collection Tool window. You can also use the printed document, Avaya Modular Messaging Data Collection Tool Online Help; see Downloading user documentation on page 12.

Do not change the data that was populated by the DCT.

⚠️ Important:

If the DCT left pane shows a red X for any item, the data is incomplete or incorrect on that screen. Click each flagged item and correct the problem before you proceed. Information must be complete and valid to continue with the migration. If you cannot fix a bad entry, do not proceed with the migration.

All account names and passwords must conform to Windows 2003 R2 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.

1. On the DCT window, click Customer details screen. The system opens the Customer details page:
   a. Complete all of the fields on this screen.
   b. Click Next.

2. Verify the settings on the Regional settings page. Click Next.

3. Verify that the message store is MSS with Avaya MAS servers. Click Next.

4. On the Voice Mail Domain screen:
   a. Verify the name for the voice mail domain (VMD).
   b. Verify the number of MASs in the voice mail domain.
   c. Click Next.

5. Verify the setting on the Corporate network details page. Click Next.
6. On the **Corporate MM server networking details** screen:
   a. Verify the server names and other settings, depending on the connection type. If necessary, fill in the IP address and the Full computer name fields.
      The DCT updates this information with each MAS that it analyzes.
   b. Click **Next**.

7. On the Corporate network details screen:
   a. Verify the domain name server (DNS), corporate default gateway, and WINS values. If the WINS field shows 127.0.0.0, change it to the correct value.
   b. Click **Next**.

8. On the **Private network** screen, verify that all the settings are correct. Click **Next**.

9. On the **Exchange message store** screen, click **Next**.

10. On the **Domino message store** screen:
    a. Select **Join the Private Windows Domain (default configuration)**.
       If the customer wants the system to move to the corporate domain, you complete this move AFTER you migrate the system. For more information, see **Moving to the corporate Windows domain after migration** on page 252.
    b. In the **Private Windows Domain name** field you can enter a new name if needed. To change the name, first select the **Change default information** checkbox and then type the new name in the field.
    c. Ignore the **Corporate Windows Domain** field.
    d. Click **Next**.

11. On the **MSS message store** screen:
    a. Select **Join the Private Windows Domain (default configuration)**.
    b. In the **Private Windows Domain name** field you can enter a new name if needed. To change the name, first select the **Change default information** checkbox and then type the new name in the field.
    c. Ignore the **Corporate Windows Domain** field.
    d. Click **Next**.

12. Verify the MSS trusted server passwords are populated.

13. Click **Next**.

14. On the **MAS accounts and passwords** screen:
    a. Enter the correct logon name for each MAS administration account.
    b. Enter the password for each account. By default, the DCT tool does not automatically insert passwords.
    c. Click **Next**.
15. On the Logon accounts and passwords screen:
   a. Enter the correct logon name and password for the technical support account and the
      customer administration account. The names and passwords must comply with the
      security standards.
   b. Click Next.

16. On the MAS service account screen, verify that Run MAS services using LocalSystem is
    selected. Click Next.

17. On the TTS and announcements screen, click Next.

18. On the MM service selection screen:

   CAUTION:
   Do not use the DCT to try to move services from one MAS to another during the
   migration! Moving services might require changes elsewhere in the system, such
   as on the MSS and in the VMSC. Move Modular Messaging services only after
   the migration is complete.

   a. Verify that the correct services are selected for each server.
   b. To activate the Web Subscriber Options (WSO) application on an MAS, click the
      appropriate column.
      You can activate Web Subscriber Options only once per voice mail domain.
   c. Click Next.

19. On the Switch Integration screen, do not change the settings. Click Next.

   CAUTION:
   When you are migrating a Modular Messaging system, you must complete the
   migration with the same PBX integration used for the previous release. Changes
   to the PBX integration can be made only after you complete the migration. For
   more information, see Changing switch integration on page 251.

20. After you have opened each DCT screen and cleared any red-flagged items, the Cancel
    button changes to a Complete button. After you have entered and verified all required data,
    click Complete. A Save window appears.

21. Save the .mmdct data file to the storage device.

22. After you save the file, the Data Collection Tool window closes.

23. Remove the storage device from the server to prevent damage to the data file.
Migrating MSS and MAS to the S8730-family server

Migrate the Message Storage Server (MSS) before you migrate any other server in the Modular Messaging system. The MSS Release 5.0 migration involves:

- [Preparing MAS#1 for the migration](#) on page 211
- [Backing up each MAS](#) on page 212
- [Backing up the MSS](#) on page 212
- [Running the Backup Verification tool](#) on page 213
- [Migrating the MSS hardware](#) on page 213
- [Restoring data on the MSS](#) on page 213
Preventing MAS#1 for the migration

Before you start the process of migration, the current Modular Messaging system must be made non-operational. Backup the data on each MAS and then backup the data on MSS.

You must prepare the first MAS for the migration before you start to migrate the MSS. These tasks are essential for a successful migration.

Busying out ports on MAS

You must not take calls during the migration. To achieve this, busy out the ports on each MAS and on the switch before you start the migration. Otherwise, messages spool on the MAS. Any spooled messages that have not been delivered to the MSS prior to performing the MSS backup will get lost. Perform the tasks as outlined in Busying out ports on each MAS on page 159 to busy out ports on the first and the subsequent MASs. This process makes the entire system inactive.

Checking the spool folder on each MAS

Before you migrate the MAS, verify that any spooled messages are delivered to the MSS:

1. Switch the monitor to show the applicable MAS.
2. Open Windows Explorer.
3. Navigate to the folder C:\Program Files\Avaya Modular Messaging\Server\Spool
4. Verify that the Spool folder contains no message files.

⚠️ CAUTION:

If the folder contains spooled messages, wait for the system to deliver them, which can take awhile.

5. When the Spool folder is empty, continue with the process of migration of MASs.
Migrating to Modular Messaging Release 5.0 on S8730-family server

----------------------------------------

**Backing up each MAS**

You must back up the data on each MAS in the system before you back up the MSS.

To back up all the data on the Modular Messaging system, first send backup data from each MAS to the MSS. The MAS information will be backed up with the MSS system data on the DVD-RAM disks. Perform the tasks outlined in [Backing up each MAS](#) on page 161.

----------------------------------------

**Backing up the MSS**

You must stop the voice system completely and backup all data from MSS to the DVD as instructed in [Backing up the MSS](#) on page 162. You must then leave the voice system out of service so that the subscribers cannot access the MSS. This is because any changes you make to mailbox or message after you take the backup will get lost.

**Note:**

Do not shut down the entire system until you complete verifying the backup data as described in [Running the Backup Verification tool](#) on page 213.
Running the Backup Verification tool

Use the Backup Verification tool after a pre-upgrade backup before continuing with the migration. To install the Backup Verification tool, see Installing the Pre-upgrade and Backup Verification tool on page 205. For more information on running the tool, see Running the Backup Verification tool on page 164.

Run the Backup Verification tool on the day you want to migrate. After you verify that every backup DVD is successful, return to the MSS main menu.

Migrating the MSS hardware

Avaya supports the following hardware migrations to an S8730:

- S3400-family or S3500-family Avaya Message Storage Server High Availability version (MSS-H) to an S8730-family MSS-H
- S3400-family or S3500-family Avaya Message Storage Server Standard Availability version (MSS-S) to an S8730-family MSS-S
- S3400-family or S3500-family MSS-S to an S8730-family MSS-H

Note:
For complete procedures to do a staged upgrade, see Avaya Modular Messaging Staged Upgrades for the Avaya Message Store Server (MSS) Release 5.0 guide.

To migrate your existing MSS to S8730-family MSS:

1. Turn off the S3400-family MSS.
2. Label all cables so you can easily reconnect them.
3. Unplug all cables to the old server.
4. Remove the S3400-family MSS from the stacked configuration or customer cabinet.
5. Install the S8730-family MSS. For more information, see Installing the Avaya S8730 Server for Modular Messaging guide.

Restoring data on the MSS

You must restore the customer data on to Modular Messaging system Release 5.0 running on S8730 server.
CAUTION:
A software restoration after a migration takes longer than a usual restore procedure, because the software does additional steps to migrate the data. Do not reboot the server until the software restoration is complete, or you will have to reload the software and restore the data again. The time required for the data restoration to complete depends on the number of subscribers in the system.

To restore data on the MSS:

1. Stop the messaging service:
   a. From the Utilities menu, click Stop Messaging.
   b. On the Stop Messaging Software page, click Stop.

      The system displays the status of stopping the messaging system.

2. After the system reports that the voice system has completely stopped, insert the DVD-RAM backup disk with the full manual backup in the DVD drive of the new hardware:

   Note:
   S8730 server does not support reading the DVD-RAM disk when it is still inside the cartridge. You must remove the disk from the cartridge to restore the backed up data onto the new server. If you have multiple backup disks, get them labeled with the correct number in sequence. Data is recorded on the unprinted side of the disk. Do not touch the unprinted side of the disk.

   Complete the following steps to safely remove the disk from the cartridge without damaging the data:
   a. Using a pointed object, break the disk locking pin. Depending on the type of disk, you might have more than one locking pin.
   b. Remove the locking pin (or pins).
   c. Unlatch the cover by using the pointed object to press the indentation on the front left-hand corner of the cartridge.
   d. Remove the disk.
   e. When placing the disk into the cartridge, ensure that the printed side of the cartridge and the printed side of the disk face the same direction.

3. Start the data restoration:
   a. From the Backup/Restore menu, click Restore.
   b. On the Restore page, set all the data types to Yes.
   c. Click Start Restore. When you see the overwrite warning, click OK.
d. On the Restore status screen, when the system prompts you to insert the first DVD, click **Continue**.

You may get the following warning message:

**The following package needs to be installed before continuing:**

```pubvt  Pre-Upgrade and Backup Verification Tools for Avaya Modular Messaging```

e. If the following appears:

1. Would you like to stop the restore and install the missing software now? [ n ];, click **Continue**.
2. Attempt to continue without updating or installing software? [ y ];, click **Continue**.

The system starts restoring all data to the system. Allow up to 40 minutes for the system to restore the data from each backup DVD. To follow the progress of the data restoration, press **Page Down** or scroll down to see the bottom of the screen.

4. After the restore is complete, reboot the system.

a. From the Utilities menu, click **Reboot Server**.

b. On the Reboot Server page, click **Reboot**.

c. At the prompt that you will lose access to the system, click **OK**.

   The reboot starts. The system displays several login prompts.

d. Ignore all login prompts until you see **Press Enter to return to prompt...**

   e. Press **Enter**.

   The login prompt appears.

5. Prepare for the next system backup:

   a. Remove the DVD-RAM backup medium from the drive. File the pre-upgrade backup DVDs in a safe place.

   b. Insert a new, writable DVD-RAM in the drive to support a Release 5.0 attended backup.

6. At the prompt, log on to the MSS as **craft**.

   The server displays the Messaging Administration web interface.

7. As a sanity check, display the Configure Network Addressing page:

   a. From the Server Administration menu, click **TCP/IP Network Configuration**.

   b. Verify the settings on this page. See **Setting up network addressing** on page 64. Verify that the corporate and private LANs are not backward.

8. From the Messaging Administration web interface, click **Subscriber Management**:

   a. Verify that the correct number of subscribers is restored. You recorded this number before backing up the MSS.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
b. On the Manage Classes-of-Service page, verify that the classes of service are correctly restored.

9. The system does not back up passwords for the remote-access login accounts. You must re-enter the correct passwords to enable remote access.
   a. From the Security menu, click **Local Administrators**.
      The system displays the Manage Local Administration Accounts page.
   b. Select an account, such as **sa** or **vm**, and then click **Edit the Selected Admin**.
      The system displays the Edit Local Administration Account page.
   c. From the Local Authentication Enabled? drop-down menu, select **yes** (if it is not already selected).
   d. For **Password**, enter the appropriate password.
   e. For **Confirm Password**, enter the password again for verification.
   f. Click **Save**.
   g. Repeat Step b for each additional login that you must administer.
   h. Set the administrative password defaults (**sa** and **vm**) and give these to the customer.
Migrating each MAS

Do this procedure on each MAS.

After you complete the migration of the MSS, you must migrate each MAS. Server migrations involve:

- Starting the MAS migration on page 217
- Preparing the new server on page 220
- Updating settings in the VMSC on page 222
- Continuing the MAS migration on page 231

Starting the MAS migration

To start migrating the MAS server:

1. Insert the storage device that contains the analyzed DCT file from your old server into the S8730 server. You must start with MAS #1.

2. Press the power button on the front of the MAS to turn on the server.

   After the MAS reboots, the Avaya Modular Messaging Configuration wizard runs automatically. The wizard uses the data file from the Avaya Modular Messaging Data Collection Tool (DCT) to configure most of the server information automatically. If for some reason the wizard does not run, contact technical support.

3. On the Welcome screen, click Next.

4. If the data file (such as sitefile.mmdct) is on the Locate Configuration Data screen, highlight the file and then click Next; otherwise, do the following:
   a. Click Browse.
   b. In the Open window, click the drop-down list next to Look in.
   c. Select the storage device, and navigate to the appropriate folder that contains the data file for this site. If the server fails to recognize the storage device, do one of the following:
      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.
   d. Double-click the correct data file for this site, such as sitefile.mmdct.
   e. On the Locate Configuration Data screen, select the correct data file.
   f. Click Next.
5. When the system prompts you to confirm the data file, click **Yes**.

The system opens Avaya Modular Messaging Data Collection Tool window.

a. If desired, page through each screen to verify the data. Click **Next** on each screen.

**Note:**
For more information about completing or verifying the data on each screen, see **Verifying DCT data** on page 207.

b. To continue the configuration process, click **Complete**.

The system automatically saves the updated data to the MISCM folder on the server.

⚠️ **CAUTION:**
Be sure to save the 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.

6. On the **Messaging Application Server Number** screen, verify that the **MAS number** field shows the correct number for this server.

- The first MAS is required. You **must** configure MAS#1 first.
- If required, change the **MAS number** field to show the correct number for this server.

7. Click **Next**.

The Configuring System screen shows the MAS configuration starting. The Sysprep window opens. The server then reboots.

8. After the reboot, 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.

**Note:**
Each Windows computer has a unique product key for the Windows 2003 R2 operating system. Enter the number exactly as shown. Record the product key.

- For a new S8730-family server, the product key sticker is located on the right-hand edge of the server chassis.
- Use only the new Windows product key received with the new S8730 and do not use the Windows product key from S3400 or S3500.

c. Click **Next**.

The Avaya Modular Messaging Configuration Wizard displays its configuration status on the Configuring System screen. The server reboots several times, but you do not need to log on manually. The entire process takes about 30 minutes.
9. If the system displays a Configuration Credential LDAP failure, verify that the MSS is running. The MSS must be available during the MAS configuration process. If the MSS is running, try the following:

- Verify that LDAP passwords in the DCT data file and on the MSS match. See Setting up the MSS local machine on page 69.
- Verify that the private network LAN cable is connected.
- If the above doesn’t work, contact support.

10. When the server configuration is complete, the progress bar stretches across the screen and the **Next** button becomes active. Click **Next**.

*Note:* If you leave the server unattended, the server can time out. If you see a message indicating that the computer is locked, press **Ctrl+Alt+Del** to log on.

11. On the Avaya Modular Messaging Wizard Completed screen, click **Finish**.

⚠️ **CAUTION:** Do not run the Avaya Modular Messaging Configuration Wizard on any subsequent server until you complete the configuration of each server in turn.
Preparing the new server

This section describes how to update and protect the new server.

Installing and administering anti-virus software

Avaya strongly recommends that anti-virus software be installed on any Microsoft Windows computer that runs Avaya Modular Messaging software. The anti-virus software used and the method of installation depends on customer requirements and the local implementation. To install the anti-virus software, use the instructions in

For more information about anti-virus software, obtain "Modular Messaging and security;" see Downloading user documentation on page 12.

Updating Microsoft Windows

A new Avaya MAS contains the most current Microsoft Windows software at the time it is shipped. After installation, you must install the latest updates for Microsoft Windows, including operating system updates and security patches. These software updates protect the system from known security weaknesses. Check with the appropriate Windows administrator for the software update procedures to use at this site.

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.
Reapply the remote access settings for each MAS

Do this task on each MAS.

Enter the IP addresses on each MAS to allow remote access:

1. Double-click the Configure icon on the desktop.
2. In the left pane of the Configure window:
   b. Expand the server name, such as MYMAS1.
3. Set up a static IP address pool as follows:
   a. In the left pane, right-click the server name, such as MYMAS1. Select Properties.
   b. In the local Properties window for the server, click the IP tab.
   c. Under IP address assignment, select Static address pool.
   d. Add or edit the address range as follows:
      ● If the window shows an incorrect IP address range, select the displayed range and click Edit. For example, the range might show all zeroes or start with 192.168.2.
      ! CAUTION: If Avaya is to support this server, do not use the preprogrammed IP addresses, such as 192.168.2.200. You must Edit or Remove these addresses for Avaya remote access to work.
      ● If no address range is already entered, click Add.
   e. In the Address Range window, enter the start and end IP addresses for this server.
   f. Verify that the number of addresses is 2.
   g. Click OK.
   h. For the Adapter field, select Allow RAS to select adapter.
   i. Click OK to close the properties window.
4. Close the Configure window.
Updating settings in the VMSC

After the migration, you must verify and update certain key settings in the Voice Mail System Configuration (VMSC) program, as described in this section.

**Note:**
The system prompts you to restart service several times during this procedure. You need to restart service only when this guide instructs you. You must restart service before entering the port board extension numbers in Configuring MAS-specific parameters on page 74. You must restart service again at the end, when configuration is complete.

Use the following steps to verify and update the following key settings:

1. In the **Voice Mail System Configuration** window, double-click the appropriate voice mail domain.

2. Verify key settings such as TUI settings, switch integration settings, and port board extensions.

3. Verify port board settings and port groups using the following steps:
   a. Double-click **Message Application Servers**.
      **Note:**
      These values are already be set. Use the most current configuration notes for this PBX integration.
   b. Expand the appropriate MAS, such as *MYMAS1*.
   c. Double-click **Telephony Interface**. Verify the port board settings for this MAS. Use the configuration notes, download the configuration notes as instructed in see Downloading configuration notes on page 11.
      **Note:**
      To verify Dialogic board configuration settings, see Appendix B: Configuring and testing port boards on page 275.
4. Update the access permissions for the Modular Messaging system:
   a. In the Voice Mail System Configuration window, expand **Security**.

   ! **CAUTION:**
   You must complete all updates to permissions in Steps b and c before you exit the VMSC. Otherwise, you can lose access to the system, and you must start over from *Migrating each MAS* on page 217.

   b. Double-click **System Administration**.
   1. Add the appropriate Modular Messaging logon accounts.

      In an MSS configuration, the Microsoft Windows **Domain Admins** account includes the other logon accounts. To add the **Domain Admins** account:
      - In the **Permissions for System Administration** window, click **Add**.
      - In the **Select Users, Computers, or Groups** window, type the first letter of the account to add in the **Enter the object names to select** box. For example, type **d** for **Domain Admins**. Click **Check Names**.
      - In the **Multiple Names Found** window, double-click the correct account.
      - Verify that the account is underlined in the list box. Click **OK**.
      - **Optional:** Repeat this task to add other logon accounts, if required.
   2. Add the Modular Messaging local service account for each server in the system.
      - In the Permissions for System Administration window, click **Add**.
      - In the Select Users, Computers, or Groups window, click **Object Types**.
      - In the Object Types window, select **Computers** so the box is checked. Click **OK**.
      - In the Select Users, Computers, or Groups window, type the first letter of the server name in the **Enter the object names to select** box. For example, type **m** for **mymas1**. Click **Check Names**.
      - In the Multiple Names Found window, double-click the server name. The **Logon Name** field shows the local account for this server in the form **MASNAME$(privdom1\masname$)**, such as **MYMAS1$(PRIVDOM1\MYMAS#1$)**.
      - Verify that the local server name is listed and underlined in the list box. Click **OK**.
      - Repeat this procedure to add the local service account for each MAS and the Supplementary server in the VMD to the System Administration ACL.
   3. Select each **Account Unknown** entry. Click **Remove**.
   4. Select the **Everyone** account. Click **Remove**.
   5. Click **OK** to close the permissions window.
Migrating to Modular Messaging Release 5.0 on S8730-family server

⚠️ CAUTION:
You must complete all updates to access permissions in Steps b and c before you exit the VMSC. Otherwise, you can lose access to the system, and you must start over from Migrating each MAS on page 217.

c. Double-click **Subscriber Administration**.

   In the Permissions for Subscriber Administration window:
   1. Add the same Modular Messaging logon accounts as you did in Step 4-b.
   2. Add the local account for each server in the system, as you did in Step 4-b.
   3. Select each Account Unknown entry. Click Remove.
   4. Select the Everyone account. Click Remove.
   5. Click OK to close the permissions window.

5. 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 States and Japan
      ● G.711 A-Law for other countries, particularly 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 H.323 and SIP integrations. G.711 encoding is required to support TTY/TDD devices.

   b. Click OK to close this window.

6. You must obtain a new RFA license for your migrated system, which includes setting up 12 TTS sessions per MAS. For instructions, see Obtaining and installing a license on MAS#1 on page 60.

7. In a multiple-MAS system, disable the Offline Access feature until all the servers are migrated. Otherwise, errors occur as the system searches for the missing offline store.

   a. For MAS#1, in the Voice Mail System Configuration window, double-click Messaging.
   b. Click the Offline Access tab.
   c. Clear the Enable offline access to messages checkbox and click OK.
   d. After all servers in the system are migrated, enable Offline Access feature again:
      1. In the VMSC window, double-click Messaging, and then click the Offline Access tab.
      2. Select the Enable offline access to messages checkbox.
      3. Click the Synchronize offline messages with remote store checkbox.
      4. Click Browse to select an existing, shared folder in the domain for the remote offline message store. The name must use the format \computername.privdom.local\
sharename, such as \mymas2.privdom.local\RemoteOfflineStore. For more information, see Creating the offline message share, if needed on page 225.

5. Click OK to close this window.

8. Complete the following steps to verify all Personal Operator Schedules:
   a. In the Voice Mail System Configuration window, double-click the appropriate voice mail domain.
   b. Double-click Telephone User Interface.
   c. Select the Personal Operator Schedules tab.
   d. Verify that all Personal Operator Schedules recorded before the migration are included in the list. If a schedule is missing, complete the following steps:
      1. Click Add.
      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 migration, which in Release 2.0 would be on the Attendant Schedules tab. Correct any discrepancies in the schedule grid.
   f. Close all windows.

Creating the offline message share, if needed

Do this task only on the server that is to host the Offline Message Store.

In a multiple-MAS system that uses the Offline Access feature, the system requires an offline message store to synchronize messages among the MASs. If the folder for offline message access is to be located on this server, you must first create the shared folder for the offline messages. The folder must be available before you can administer the Offline Access feature.

To create a shared folder for offline messages with the correct permissions:

1. Using Windows Explorer, create a new folder on this server. For example, create RemoteOfflineStore on the C: drive.
2. Right-click the folder name and select Sharing and Security.
3. In the Properties window, on the Sharing tab:
   a. Select Share this folder.
   b. Verify the Share name, such as RemoteOfflineStore.
   c. Click Permissions.
   d. In the Permissions window, verify that the Everyone account exists. If it does exist, continue with step 4. If the Everyone account does not exist, do the following to add it:

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Migrating to Modular Messaging Release 5.0 on S8730-family server

1. In the Permissions window, click **Add**.
2. In the Select Users, Computers, or Groups window, type the first letter of the account to add in the **Enter the object names to select** box.
   For example, type **e** for **Everyone**.
3. Click **Check Names**.
4. In the Multiple Names Found window, double-click the correct account.
5. Verify that the account is listed and underlined in the list box.
6. Click **OK**.
7. **Optional**: Repeat this task to add other logon accounts, if required.
8. Give the correct share permissions to the accounts. In the Permissions window:
   - Select each account in turn.
   - In the **Permissions** box, under **Allow**, select the permissions **Change** and **Read**, so the boxes are checked.
   - Repeat this task for each logon account.
9. Click **OK** to close the Permissions window.

4. In the **Properties** window, click the **Security** tab.
   a. Click **Add** and add all Modular Messaging computer accounts that will access the offline storage server:
      1. In the Select Users, Computers, or Groups window, click **Object Types**.
      2. In the Object Types window, select **Computers** so the box is checked. Click **OK**.
      3. In the Select Users, Computers, or Groups window, type the first letter of the server name in the Enter the object names to select box. For example, type **m** for mymas1.
      4. Click **Check Names**.
      5. In the Multiple Names Found window, double-click the server name.
         The Logon Name field shows the local account for this server in the form MASNAME$(privdom1\masname$), such as MYMAS1$(PRIVDOM1\MYMAS#1$).
      6. Verify that the local server name is listed and underlined in the list box. Click **OK**.
      7. Repeat this procedure to add a local service account for each server in the system.
   b. Give the correct share permissions to these accounts. In the **Properties** window:
      1. Select each account in turn.
      2. In the **Permissions** box, under **Allow**, select the following permissions so the boxes are checked:
         - Modify
         - Read & Execute
Migrating each MAS

- List Folder Contents
- Read
- Write

3. Repeat this task for each logon account and each MAS computer account.

5. Click OK to close the Properties window.

6. Reboot each MAS in the system for the offline access permissions to take effect.
Restarting messaging services

After you verify and update all required settings, you must restart the messaging service for the configuration changes to take effect. Verify that the system is working.

To restart messaging service:

1. Double-click the Monitor icon on the desktop.
2. Click Services (Local) in the left pane, if the item is not already selected.
3. Restart messaging 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.

   **CAUTION:**
   Do not select the Restart option. Always stop, and then start, as described.

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

   The system restarts the messaging service.

**Note:**

When you restart messaging service, the Monitor window displays the status of the service as Started. However, the service might 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. In the left pane, expand Event Viewer (Local), and then click Application.
      2. Refresh the window display periodically until you see Telephony User Interface event 1241, TUI service has been enabled. You can then proceed.

4. Verify that the correct 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. These services start with the abbreviation MM. Verify that the Status column shows the correct state for each messaging service:
      - The following services, see Table 7, are automatically installed on every MAS. Enable them based on the information in the table.
      - Services that are required for this server must show Started and a startup type of Automatic.
Migrating each MAS

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

Table 7: Enabling Modular Messaging services in a VMD

<table>
<thead>
<tr>
<th>Modular Messaging service name</th>
<th>Condition for enabling service</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM Messaging Application Server</td>
<td>Enable on each MAS and on the Supplementary server, if present.</td>
</tr>
<tr>
<td>MM Service Connector</td>
<td></td>
</tr>
<tr>
<td>Avaya SPIRIT</td>
<td></td>
</tr>
<tr>
<td>MM Alarming Server</td>
<td></td>
</tr>
<tr>
<td>MM Audit Service</td>
<td></td>
</tr>
<tr>
<td>MM Event Monitor Server</td>
<td></td>
</tr>
<tr>
<td>MM Fault Monitor</td>
<td></td>
</tr>
<tr>
<td>MM Performance Monitor Server</td>
<td></td>
</tr>
<tr>
<td>MM Process Monitor Server</td>
<td></td>
</tr>
<tr>
<td>MM Call Me 1</td>
<td>Enable on only one server in each VMD, either on an MAS or the Supplementary server, if present.</td>
</tr>
<tr>
<td>MM Fax Sender 2</td>
<td>See the Avaya Modular Messaging Concepts and Planning Guide for the recommended load balancing of services between multiple servers.</td>
</tr>
<tr>
<td>MM Mailbox Monitor 2</td>
<td></td>
</tr>
<tr>
<td>MM MWI 2</td>
<td></td>
</tr>
<tr>
<td>MM Tracing Service</td>
<td></td>
</tr>
</tbody>
</table>

1. The Call Me, MWI, and Mailbox Monitor services must always be enabled on the same server.
2. IP H.323 switch integration does not support fax service.

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**.
   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** before you do Step d. Serious problems occur if you activate a service that is supposed to run on only one server in the VMD on multiple servers.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Migrating to Modular Messaging Release 5.0 on S8730-family server

d. If the Status for any MM service that is required for this server is Stopped or blank:
   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, repeat Step d.

5. When configuration is complete, close all open windows.

6. For a multiple-MAS system, after you configure the last MAS, restart MM services on all servers in the VMD. A restart ensures that the voice mail domain-wide properties are consistent across the VMD. To restart MM services on all MASs in the voice mail domain:
   a. Switch the monitor to show the next MAS in the system.
   b. Repeat Steps 3 through 5 under Restarting messaging services on page 228 to restart messaging service.
   c. Repeat this step (6) for each MAS in the system.

Completing VMSC setup

Complete the following for the current MAS:

1. Enter product IDs for the current MAS; see Entering Product ID for current MAS on page 63.

2. 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 migration. For additional information, see Configuring serviceability settings on MAS#1 on page 58.

3. Configure the following services as applicable:
   a. MM Audit Service; see Configuring MM Audit Service on page 67.
   b. MM Fax Sender server; see Configuring the MM Fax Sender server on page 68.

4. Verify each service:
   a. MM Audit Service; see Verifying Audit service on page 83.
   b. MM Fax Sender server; see Creating and printing a fax message on page 127.
Completing MSS administration

Continuing the MAS migration

After you migrate an MAS, continue as appropriate:

- For MAS#1, continue the migration all the way through Completing MSS administration on page 231. If you restore the data onto MAS#1 and redeploy the caller applications, all subsequent MASs will automatically get the deployed Caller Applications.

- For subsequent MASs and Supplementary server:
  1. Ensure that the most current data file is on the storage device.

  **CAUTION:**
  When you update any information in the DCT data file, save the updated file to the storage device. You must use the most current copy for subsequent server migrations. Copy the most recent DCT data file to the storage device:

  2. Configure each MAS:

     - If you have another MAS or Supplementary server, continue with Migrating each MAS on page 217.

     - If all MASs and Supplementary servers are now migrated, continue with Restoring data on each MAS on page 234.

Completing MSS administration

Complete the following tasks on the MSS:

- Verify the MAS host information on page 232
- Placing the MSS in the Windows domain—MAS#1 only on page 233

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Verify the MAS host information

Repeat this task for each MAS you migrate.

MSS updates the host information, and then sends the updated information to all MASs in the Modular Messaging system as outlined in Updating MAS host information on page 103. Verify that all servers that are currently in the Modular Messaging system are updated.

1. On the Messaging Administration web interface, click Server Administration> MAS Host Send.
   The system displays the Send MAS Host Information page.
2. Click Send.
   The system sends the host information to all MASs at the same time and reports whether the information was updated successfully.
Placing the MSS in the Windows domain—MAS#1 only

Do this task only once per each migration, after you migrate MAS#1.

Because you reloaded the software on MAS#1, you must add the MSS to the created Windows domain.

To add the MSS to the private Windows domain:

1. From the Server Administration menu, click Windows Domain Setup.
   The system displays the Windows Domain Setup page.

2. Enter the following information in each field:
   a. For MSS NetBIOS Name, type the MSS private system name, which is mss1.
   b. For NetBIOS Domain Name, type the NetBIOS domain name for the private Windows network that was created on MAS#1, such as privdom1.
   c. For Fully Qualified Domain Controller Name, type the full computer name for MAS#1 on the private network, such as mymas1.privdom1.local.

   ! CAUTION:
   In the following step, you must enter the current account name and password for the MAS administrator or else MAS backups will fail. You must use the same account to set up system backups on each MAS. For more information, see Backing up the system on page 139.

   d. For Account For Joining The Domain, type the domain administrator account name, such as dom-admin.
   e. For Password For Joining The Domain, type the password for this account.

   Note:
   At this time make sure that the User Corporate LAN? checkbox is blank.

   If joining the MM system to the corporate Windows domain DO NOT select Use Corporate LAN? checkbox at this time. You need to return after completing the corporate Windows domain setup and check this field.

   If the system will remain on the private Windows domain, ensure that the Use Corporate LAN? check box is clear.

3. Click Save.
   The page displays the Windows domain setup status.
Restoring data on each MAS

Restore the backed-up data onto each MAS.

This section includes the following topics:

- Stopping all MM services on page 235
- Restoring backed-up MAS data on page 236
- Restoring Caller Applications—MAS#1 only on page 238 —required on MAS#1 only
- Restarting Modular Messaging services on page 239
- Installing software updates on page 240
- Updating Microsoft Windows on page 49
- Performing acceptance tests for a migration on page 241
Stopping all MM services

To stop all Modular Messaging services:

1. Switch the monitor to show the correct 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 Intel 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, if the item is not already selected.
   c. If the Monitor window was already open, refresh the screen.
   d. In the right pane, scroll down to the list of installed Modular Messaging services. These
      all start with the abbreviation **MM**.
   e. Verify that the **Status** column is blank. If any service is **not** stopped, repeat Steps 2 and
      3.
Restoring backed-up MAS data

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

To restore the backed-up MAS data:

1. Map to the backup drive for this MAS on the MSS:
   a. On the desktop, right-click the My Computer icon and select Map Network Drive.
   
   **Note:**
   If you renamed the icon label, the computer icon shows the server name, such as mymas1.
   
   b. In the Map Network Drive window, in the Folder field, type \mss1\masbackup.
   
   c. Clear the Reconnect at logon checkbox.
   
   d. Click Connect using a different user name.
   
   e. In the Connect As window, for User name, enter the private Windows domain name and the domain administrator account name in the format domain\account name. For example, type privdom1\dom-admin.
   
   f. Enter the password for this account. Click OK.
   
   g. In the Map Network Drive window, click Finish.
   
   The system opens a window to the designated drive letter, such as Z:

2. Double-click the Backup icon on the desktop.

3. In the Backup Utility window, on the Welcome tab, click Restore Wizard.


5. On the What to Restore screen, click Browse.
   a. In the Open Backup File window, click Browse.
   
   b. In the Select file to catalog window, under Look in, navigate to the mapped drive.
   
   c. Double-click the backup file for this MAS. For example, MYMAS1DailyBackup.bkf.
   
   d. In the Open Backup File window, click OK.
   
   The system returns to the What to Restore screen.

6. Verify that the system displays the full name of the MAS backup file in the right pane under Media Location. For example, Z:\MYMAS1DailyBackup.bkf.
7. In the left pane under **Items to restore**, expand **File**.
   a. Expand the correct entry for the daily backup of this MAS. The file uses the naming convention from the previous software release, such as *Daily Backup of MYMAS1*.
   b. Expand C:.
8. Select the folders and files to be restored:
   a. Select the checkbox next to **Avaya Support** so that the box is checked. This folder includes the Tone_Files folder, which contains any custom tone files.
   b. Expand the folders **Program Files > Avaya Modular Messaging > VServer**.
   c. Select the checkbox next to **VServer** so the box is checked.
   
   **CAUTION:**
   Do not restore the System State! You also do not need to restore the hosts file, because you already resent the most current version from the MSS.
   d. Click **Next**.
9. On the Completing the Restore Wizard screen, click **Advanced**.
   a. On the Where to Restore screen, select **Original location**. Click **Next**.
   b. On the How to Restore screen, select **Replace existing files**. Click **Next**.
   c. On the Advanced Restore Options screen, verify the following settings:
      1. Clear the checkboxes for **Restore security setting** and **Restore junction points, not the folders and file data they reference**.
      2. Leave **Preserve existing volume mount points** selected.
      3. Click **Next**.
10. On the Completing the Restore Wizard screen, review the restore information. Click **Finish**.
    The Restore Progress window displays restore information.
11. When the data restoration is complete, close the Restore Progress window.
13. If the system asks if you want to restart, select to restart.
14. Close the mapped drive window, such as Z:.

   **CAUTION:**
   You *must* disconnect the mapped drive, or automatic nightly backups might fail.
15. Disconnect the mapped drive:
   a. On the desktop, right-click the **My Computer** icon and select **Disconnect Network Drive**.
   b. In the Disconnect Network Drives window, under **Network Drives**, select \mss1\masbackup. Click **OK**.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Restoring Caller Applications—MAS#1 only

Do this task only on MAS#1.

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

1. Click Start > Run to open a Command prompt window.
2. In the Run window Open field, type the following and press Enter:

```
C:\Avaya_Support\CMD\CARestore.bat
```

A command window opens. The script shuts down all Modular Messaging services, and copies the Caller Applications to the server. The script takes a few seconds to run.

Note:

The system deploys Caller Applications automatically after migration. Restore the Caller Applications on MAS#1 before you migrate any subsequent MASs. The additional MASs then have the Caller Applications automatically.
Restoring data on each MAS

Restarting Modular Messaging services

After you restore the data, you must restart the Modular Messaging services for this MAS.

1. To restart Modular Messaging services:
   a. Click Start > Run to open the Run window.
   b. In the Open field, enter the following text and press Enter:

   C:\Avaya_Support\Scripts\serverrecovery.vbs

   The script takes a few seconds to run.

2. Verify that all the Modular Messaging services required for the MAS are started:
   a. Double-click the Monitor icon on the desktop or from the command prompt run services.msc.
   b. Click Services (Local) in the left pane, if the item is not already selected.
   c. If the Monitor window is already open, refresh the screen.
   d. 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 for this server must show a blank status and a startup type of Disabled. For more information, see Restarting messaging services on page 228.
   e. If the Status for any MM service that is required for this server is Stopped or blank, repeat Steps 1 and 2.

   The system starts a messaging service startup.
   f. Track the startup progress as follows:

   1. In the left pane, expand Event Viewer (Local), and then click Application.
   2. Refresh the window display periodically until you see Telephony User Interface event 1241, TUI service has been enabled. You can then proceed.
   g. Close the Monitor window.

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

The Modular Messaging Release 5.0 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.

Complete the following steps to update Modular Messaging software:


   **Note:**
   If you followed the procedure for Downloading software updates on page 10, you already downloaded any required software updates.

2. Follow the instructions provided in Updating Modular Messaging software on page 323 to update the system with the latest changes before you do acceptance testing.
Performing acceptance tests for a migration

To verify that the migrated system is working correctly:

1. Continue with Running acceptance tests on page 120.

2. Do all acceptance tests that are appropriate for each server. For example:
   - For an MAS, test that the server can send and receive calls.
   - For all servers, verify that the services installed on that server are working. For example, if Message Waiting Indication (MWI) or Tracing Service is installed on a server, verify that these services work.

If you have migrated all MASs and Supplementary servers, continue with Completing the system migration on page 242.
Completing the system migration

Complete the migration of Modular Messaging system as follows:

- Running a DCT analyze on the migrated system on page 242
- Backing up the system on page 242
- Completing the Modular Messaging system migration on page 247
- Updating or installing client software on page 248

Running a DCT analyze on the migrated system

Use the DCT to analyze the migrated system; see Using the DCT to analyze the current configuration on page 136.

Back up the system

After the migration, back up the Modular Messaging system to save the new Release 5.0 data. First back up each MAS. Remove old backup files to free up space, and then back up the MSS.

Running backups on each MAS

Do this task on each MAS and the Supplementary server, if present.

To back up the Release 5.0 data on each MAS:

1. Switch the monitor to show the correct MAS.
2. Double-click the Scheduled Tasks icon on the desktop.
3. In the Scheduled Tasks window, run an attended backup on this MAS:
   a. Right-click the MAS Backup task that is already set up.
   b. Select Run.

   The system immediately starts to back up the data on this MAS to the MSS. The Status column shows Running. When the backup is complete, the Status column goes blank. This backup takes about one minute.
4. Optional: To verify the success of the backup:
   a. Double-click the **Monitor** icon on the desktop.
   b. In the left pane, expand **Event Viewer (Local)**, and then click **Application**.
      1. Refresh the window display periodically until you see the following events:
         - **ntbackup 8009, End Verify of C:**
         - **ntbackup 8019, End Operation: The operation was successfully completed.**
   
   **Note:**
   On MAS#1, the event viewer shows two sets of backup events because the backup program generates two files on the MSS: *MYMAS#1MASSingle.bkf* and *MYMAS#1MASAll.bkf*. Backups on subsequent MASs generate only the MASAll.bkf file for each MAS, so only one set of backup events is present.
   c. If the backup fails to run, verify the account settings:
      1. Double-click the task **MAS Backup** to view the properties window.
      2. In the MAS Backup window, click the **Task** tab. Verify that the account in the **Run as** field is the correct account that has permissions to run backups manually, such as *privdom1\dom-admin*. If the account is incorrect, type the correct value now. For more information, see Placing the MSS in the Windows domain—MAS#1 only on page 233.
      3. If you change the account, or to verify the password, click **Set password**. In the Set Password window, enter and confirm the password for the required account. Click **OK**.
      4. Click **OK** to close the MAS Backup window.
      5. Repeat Step 3a to run the backup again.
   5. Close the **Scheduled Tasks** window.
   6. Repeat this procedure for each MAS in the system.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Removing old backup files from the MSS

The Modular Messaging backup file names may have changed from the release that your system was running to Release 5.0. You must remove the old backup file from each MAS in the system so it does not use up valuable disk space on the MSS.

⚠️ **CAUTION:**

Do not remove the old backup files until you confirm that data restoration is complete and that the new MAS backup procedure is working.

To remove the old backup files from each MAS:

1. Switch the monitor to show the MAS.
2. Map to the backup drive on the MAS:
   a. On the desktop, right-click the **My Computer** icon and select **Map Network Drive**.
   
   **Note:**
   
   If you renamed the label, the computer icon shows the server name, such as *mymas1*.
   
   b. In the Map Network Drive window, in the **Folder** field, type `\mss1\masbackup`.
   
   c. Clear the **Reconnect at logon** checkbox.
   
   d. Click **Connect using a different user name**.
   
   e. In the Connect As window, for **User name**, enter the Windows domain name and the domain administrator account name in the format `domain\account name`. For example, type `privdom1\dom-admin`.
   
   f. Enter the password for this account. Click **OK**.
   
   g. In the Map Network Drive window, click **Finish**.
   
   The system opens a window to the designated drive letter, such as Z:\.
3. In Windows Explorer, locate the backup file for the pre-migrated system on the MSS. The old backup file is at least 264 MB in size and uses the format `MYMASDailyBackup.bkf`, where `MYMAS` is the host name of the MAS.

⚠️ **CAUTION:**

The following backup files support Release 5.0. Do not delete any of the following files, where `MYMAS` is the host name of the MAS.

- `MYMAS#1MASSingle.bkf` contains deployed Caller Applications data for the system, the *.uma files. Only MAS#1 generates this file.

- `MYMAS#MASSingle.bkf` contains tone files, custom prompts, and PBX configuration information. Each MAS in the system generates its own MASAll.bkf file.
4. Delete the old backup file for this MAS:
   a. Right-click the old backup file, such as *MYMASDailyBackup.bkf*. Select **Delete**.
   b. When the system prompts you to confirm the deletion, click **Yes**.
   c. Close the window to the mapped drive.
5. Disconnect the mapped drive:
   a. On the desktop, right-click the **My Computer** icon and select **Disconnect Network Drive**.
   b. In the Disconnect Network Drives window, under **Network Drives**, select \mss1\masbackup. Click **OK**.

   **Note:**
   You **must** disconnect the mapped drive, or automatic nightly backups might fail.
6. Repeat this task for each MAS in the system.

**Backing up the MSS**

After you have run an attended backup of each MAS, run an attended backup on the MSS now. Make the first system backup to DVD-RAM.

1. Log on to the MSS server as **craft** using the appropriate password.
   The system displays the Messaging Administration web interface.
2. Insert a labeled, writable DVD-RAM into the DVD drive for the system backup.
3. To run an attended backup, from the Backup/Restore menu, click **Backup**.
   The system displays the Backup page.
4. Make a backup of the new Release 5.0 system data:
   a. Because the system is not yet in service, you do not have to stop the voice system.
   b. Verify that **Media Type** is set to **DVD-RAM**.
   c. Set all the data fields to back up to **Yes**.
   d. Click **Start Backup**.
   e. If the system prompts you to continue, click **Continue**.
   f. The system estimates the number of DVDs that it requires. Verify that you have the correct number of DVDs available. Click **Continue**.
   g. When the system prompts you to insert the DVD, click **Continue**.
      The system saves the new system configuration to the DVD. Allow about 30 minutes for each DVD.
   h. Follow the prompts on the screen to track and complete the backup process. Scroll to the bottom of the page to see the most recent status messages. The message

   **Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.**
FULL-MANUAL BACKUP completed successfully indicates that the backup is complete.

5. After the backup is complete, restart the messaging service:
   a. From the Utilities menu, click Start Messaging.
   b. On the Start Messaging Software page, the system displays the status of starting the messaging system. Verify that voice messaging restarts.

6. After the backup is complete, leave the DVD-RAM backup medium in the DVD-RAM drive to support the next unattended backup.

7. Consult with the customer about the method to use at this site for running regular unattended (scheduled) backups of the system data.

   The system supports backups to DVD-RAM or through the customer network using FTP/SFTP. For instructions, obtain “Backing up the MSS,” see Downloading user documentation on page 12. For overview information, see Avaya Modular Messaging Concepts and Planning Guide.
Completing the Modular Messaging system migration

Use the following steps to complete the Modular Messaging system migration:

1. Connect any disconnected modems to restore normal alarming for the Modular Messaging system.

2. Review event and alarm logs and resolve any problems; see the Avaya Modular Messaging MAS Administration Guide.

3. On the Messaging Administration web interface, complete the following:
   a. Under the Alarming menu, click Alarming Configuration.
      The system opens Configure Alarms page.
   b. In the Alarm Suppression field, click INACTIVE.

4. On the MAS, enable 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, clear the Suppress alarm notifications check box to turn it on the alarm notifications options.
   d. Close all windows.

5. If you are adding a new MAS to the system, install the new server now.
   - Print Modular Messaging on Avaya MAS installation checklist on page 254 or Modular Messaging on a customer-provided MAS installation checklist on page 260 as appropriate and use as a guide.
   a. Install the new server. For more information, see Installing the Avaya S8730 Server for Modular Messaging guide.
   b. Update the DCT data file, configure the new server, and redistribute the Modular Messaging services to all installed servers.
   c. Send a copy of the most current DCT data file to the appropriate technical support group. Afterwards, erase the data file from your storage device for security purposes.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Updating or installing client software

After the Modular Messaging system migration is complete, you might need to update or install new client software. Client software includes:

- Modular Messaging Web Client—*must* be on its own server, *not* on an MAS or a Supplementary server
- Modular Messaging Web Subscriber Options, if installed on a non-MAS server
- Avaya Modular Messaging Notes Client
- Avaya Modular Messaging Outlook Client, Avaya Modular Messaging Outlook Restricted Client, Subscriber Options.

Note that *Subscriber Options components* are installed automatically on the MAS as part of the migration to Release 5.0. *Do not* manually install or delete any MM Clients, including Subscriber Options. For more information, see the *Avaya Modular Messaging Subscriber Options User Guide*; see *Downloading configuration notes* on page 11.

- Mailbox Manager
Reducing servers by replacing S3400 servers with S8730 servers

This upgrade scenario describes how to reduce the number of MASs in your VMD by replacing S3400-family servers with S8730 family servers.

**Note:**
Use this procedure only to reduce the number of S3400 MASs.

The modular Messaging system in this example has four S3400-family server MASs, each running 23 ports of T1 QSIG. You are upgrading to Release 5.0 so the customer is required to use the S8730-family servers. 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 will fail. Which means you must consolidate and configure the T1 QSIG port boards into two MASs for the current S3400-family 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 277.
   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.

2. Remove MAS#3 and MAS#4 as Trusted Servers from the MSS:
   a. At the MSS prompt, log on as **craft**.
      The server displays the Messaging Administration web interface.
   b. Click **Trusted Servers**.
   c. On the Manage Trusted Servers page, click **Delete the Selected Trusted Server** to remove the Trusted Server information for MAS#3 and MAS#4.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
3. Remove the MAS host information for MAS#3 and MAS#4:
   a. From the Server Administration menu, click **MAS Host Setup**.
   b. Click **Remove** to remove the Host information for MAS#3 and MAS#4.

4. Remove MAS#3 and MAS#4 from the VMD:
   a. Sign onto MAS#3 as **craft**.
   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-family 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 MSS and in the VMSC. Move Modular Messaging services only after the migration is complete.

5. Obtain and run the DCT (mmdct.exe) to collect data and analyze the remaining S3400 MASs; see **Using the DCT to collect information from an MAS** on page 206.

6. Continue with the migration to Release 5.0; see **Migrating MSS and MAS to the S8730-family server** on page 210.
Changing switch integration

The switch integrations may use different Dialogic port boards or may not use a Dialogic port board. If you are changing the switch integration as part of the migration procedure, the system does not restore the configuration for switch configuration and Dialogic port boards. Therefore, you must manually configure them. Use the procedures described in Configuring port boards and switch integration on page 75 and procedures described in Configuring and testing port boards on page 275.

If you have to change the switch integration while migrating the Modular Messaging system to Release 5.0, you must first complete the migration of the MSS and all of the MASs using the procedures outlined in this chapter.

You do not have to perform this procedure if you are not changing switch integration. The migration process restores the initial switch configurations.
Moving to the corporate Windows domain after migration

After you migrate to Release 5.0, you can move the Avaya Modular Messaging system to the customer’s corporate Windows domain. This option is beneficial to customers who do not want a separate private Windows domain within their network. For complete procedure to move the Avaya Modular Messaging system to the corporate Windows domain, see Moving to the corporate Windows domain after upgrade on page 188.
Appendix A: Installation and upgrade checklists

This appendix provides checklists to help guide you through the various installation, upgrades and migration tasks.

- Before you start a new Modular Messaging installation or upgrade, print the checklist relevant to the procedure that you must do.
- Check off the steps as you complete to ensure that you do not miss any important task.

**Note:**
If you want to add a new MAS to an existing Modular Messaging system, upgrade the software *first* if one is required. Install the new MAS using the new installation checklist.

Checklists include:

- **New Installation**
  - [Modular Messaging on Avaya MAS installation checklist](#) on page 254
  - [Modular Messaging on a customer-provided MAS installation checklist](#) on page 260

- **Upgrades and migration**
  - [Modular Messaging Release 5.0 upgrade and migration checklists](#) on page 265
    - [Modular Messaging Release 3.x or 4.0 on S3500-family server upgrade checklist](#) on page 266
    - [Modular Messaging Release 5.0 system migration checklist](#) on page 269

- **Moving Modular Messaging system after an upgrade or migration**
  - [Moving the MM system to the corporate Windows domain checklist](#) on page 274
Modular Messaging on Avaya MAS installation checklist

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

<table>
<thead>
<tr>
<th>✔ Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete preinstallation planning:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If Avaya is to maintain this system, pre-register each MAS in ART to obtain</td>
<td></td>
<td>You can obtain the required information for</td>
</tr>
<tr>
<td>the server product ID and IP addresses for remote access.</td>
<td></td>
<td>each MAS in advance.</td>
</tr>
<tr>
<td>Obtain the DCT data file for this site.</td>
<td>9</td>
<td>Local procedures vary.</td>
</tr>
<tr>
<td>Assemble and review the required documentation.</td>
<td>9</td>
<td>Web access required.</td>
</tr>
<tr>
<td>Download any required Avaya software updates (including Outlook Client,</td>
<td>10</td>
<td>Web access required.</td>
</tr>
<tr>
<td>DCT Tool, and the Pre-upgrade and Backup Verification Tool).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain user documentation.</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Review security issues.</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Obtain the required anti-virus software for the MAS.</td>
<td>14</td>
<td>Customer gets the needed software.</td>
</tr>
<tr>
<td>Collect any software media that is needed for the installation,</td>
<td>14</td>
<td>Leave customer DVDs on-site.</td>
</tr>
<tr>
<td>such as Microsoft Windows updates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gather the necessary test equipment.</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Gather the necessary tools for installation.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for</td>
</tr>
<tr>
<td>Arrive for LAN administration of the Modular Messaging system. Register</td>
<td>15</td>
<td>Modular Messaging guide.</td>
</tr>
<tr>
<td>MAS and MSS corporate computer names on the DNS.</td>
<td></td>
<td>See LAN administrator.</td>
</tr>
<tr>
<td>Note: Avaya Inc. is not responsible for the installation, administration,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>or test of communications between customer PCs and the LAN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify that the PBX or switch is administered.</td>
<td>15</td>
<td>See switch administrator.</td>
</tr>
<tr>
<td>Create user accounts in the corporate Windows domain.</td>
<td>17</td>
<td>Only for systems that join the corporate</td>
</tr>
<tr>
<td>Perform user by the corporate domain admin.</td>
<td></td>
<td>Windows domain.</td>
</tr>
</tbody>
</table>

Table page 1 of 6
## Modular Messaging on Avaya-provided MAS installation checklist

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create computer accounts in the corporate Windows domain. Performed by the corporate domain admin</td>
<td>18</td>
<td>Only for systems that join the corporate Windows domain.</td>
</tr>
<tr>
<td>Review preinstallation site requirements, including:</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>● Environmental requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Weight and space considerations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Customer-provided cabinet requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Installation area requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Power and grounding requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Demarcation points</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install the hardware: For complete information on how to install Avaya S8730 server and its accessories, see Installing the Avaya S8730 Server for Modular Messaging guide.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify each S8730-family server in the system.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>Unpack the Modular Messaging system hardware and peripheral components.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>Attach mounting brackets and handles to the UPS and any EBM (extended battery module) units as needed, and then cable the units together.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>Attach rails for rack-mount or rubber spacers for stackable configuration to each Avaya server.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>Connect the power cables for the system.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>Connect the MAS port boards, if present, to the PBX.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>Set up the MSS and MAS private LAN using an Ethernet crossover cable.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>Connect a multiple-MAS system using an Ethernet switch:</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>● Connect the MSS and first MAS only to the Ethernet switch for the private LAN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Connect each server to the corporate LAN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install an optional KVM switch.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
</tbody>
</table>
## Modular Messaging on Avaya-provided MAS installation checklist

<table>
<thead>
<tr>
<th>✓ Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up the optional external modem for the MSS.</td>
<td></td>
<td>See <em>Installing the Avaya S8730 Server for Modular Messaging</em> guide</td>
</tr>
<tr>
<td>Set up the optional external modem for each MAS.</td>
<td></td>
<td>See <em>Installing the Avaya S8730 Server for Modular Messaging</em> guide</td>
</tr>
<tr>
<td>Turn on the Modular Messaging system and peripheral components.</td>
<td></td>
<td>See <em>Installing the Avaya S8730 Server for Modular Messaging</em> guide</td>
</tr>
</tbody>
</table>

**Do initial MSS administration:**

<table>
<thead>
<tr>
<th>✓ Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log on to the MSS.</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Adjust the monitor settings if needed.</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>Start the MSS configuration using a DCT data file. If you want to configure the MSS manually, use procedures in</td>
<td>24</td>
<td>Must do manually before configuring an MAS</td>
</tr>
<tr>
<td>Set the time and date</td>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>

**Prepare for corporate Windows domain installs—perform this section only if the MM system is joining the corporate Windows domain:**

<table>
<thead>
<tr>
<th>✓ Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create user accounts in the corporate Windows domain (performed by the corporate domain administrator).</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Create computer accounts in the corporate Windows domain (performed by the corporate domain administrator).</td>
<td>18</td>
<td></td>
</tr>
</tbody>
</table>

**Configure the MAS—repeat this section for each MAS and the Supplementary server:**

<table>
<thead>
<tr>
<th>✓ Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch the monitor to show the correct MAS.</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>Complete MAS configuration prerequisites.</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>In the Modular Messaging configuration wizard, locate the data file for the Data Collection Tool (DCT).</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>Enter or verify the data in the DCT data file.</td>
<td>44</td>
<td>Do if required.</td>
</tr>
<tr>
<td>Install and administer anti-virus software.</td>
<td>48</td>
<td>Local procedures vary.</td>
</tr>
<tr>
<td>Install the latest Avaya-approved updates for Microsoft Windows: system updates and security patches.</td>
<td>49</td>
<td>Local procedures vary.</td>
</tr>
<tr>
<td>Enter the correct RAS IP addresses to allow remote access.</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>

Table page 3 of 6
## Modular Messaging on Avaya-provided MAS installation checklist

<table>
<thead>
<tr>
<th>✓ Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Configure and test the port boards if required, including:  
  ● For analog boards, create or use a valid tone file.  
  ● Configure each port board.  
  ● Test incoming and outgoing calls on each board. | 52 | Configuration notes required. Skip this step for IP-type or automatically configured integrations. |
| Verify that the preferred language for administration. | 55 | |
| Verify that Modular Messaging services has started. | 55 | Do these tasks on MAS#1. Configuration notes required for PBX settings. |
| Use the Voice Mail System Configuration (VMSC) program to configure required domain-wide settings on MAS#1:  
  ● TUI and administration access settings  
  ● PBX parameters using the configuration notes  
  ● Serviceability settings for Modem Dialout, SNMP, or Internet alarming  
For MultiSite specific configuration, see **Voice Mail System Configuration** section in *Avaya Modular Messaging Release 5.0 with the Avaya MSS MAS Administration Guide*. For information on MultiSite concepts and requirements, see *Avaya Modular Messaging MultiSite Feature Description Guide*. | 56 | |
| Use the VMSC to get the VMD ID needed for the license and submit the request. Install the license file after delivery and set up TTS sessions for each MAS. | 60 | Local procedures vary. |
| Enter Product ID for current MAS. | 63 | Set up the features and services that are required on each MAS or on the Supplementary server. |
| Configure the Call Me, Notify Me, MWI, Audit, Fax, language or TTS, and offline access (do OLA only on the last server).  
Reconfigure any of these services that are not enabled or are enabled on the wrong server. | 64 | |
| Configure specific parameters for this MAS, including:  
  ● Modem Dialout alarming, if used  
  ● Port boards and switch integration settings using the configuration notes. | 74 | Do for each MAS. Configuration notes required. |
| Restart the messaging services on all MASs in the VMD as a final step.  
  ● Verify that the services that are not required on this MAS are disabled. *Do not* start all MM services until this is done.  
  ● Verify that all MM services required on this server are started and set to **Automatic**. | 77 | Ensure that the correct services are enabled on each MAS. |
| Verify the ability of each MAS to handle calls. | 80 | Not applicable for Supplementary server. |
| Verify the alarming setup on each MAS. | 81 | |

Table page 4 of 6

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
### Modular Messaging on Avaya-provided MAS installation checklist

<table>
<thead>
<tr>
<th>✓ Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Tracing Service operation, if installed on any server.</td>
<td>82</td>
<td></td>
</tr>
<tr>
<td>Verify Audit Service</td>
<td>83</td>
<td></td>
</tr>
<tr>
<td>Add the Supplementary server name into the security configuration</td>
<td>62</td>
<td>Applicable only for Supplementary server.</td>
</tr>
<tr>
<td>Complete initial MSS administration:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch the monitor to show the MSS.</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Continue the MSS configuration using a DCT data file</td>
<td>102</td>
<td></td>
</tr>
<tr>
<td>Configure the MSS modem</td>
<td>115</td>
<td></td>
</tr>
<tr>
<td>Install any software updates, if needed</td>
<td>116</td>
<td></td>
</tr>
<tr>
<td>Do acceptance tests:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set up the monitoring tools such as the operational history viewer, and port monitor for multiple-MAS systems to track the calls.</td>
<td>118</td>
<td>Useful for troubleshooting.</td>
</tr>
<tr>
<td>Do acceptance tests on each MAS, including:</td>
<td>120</td>
<td>Tests vary per MAS and local system setup.</td>
</tr>
<tr>
<td>● Create and receive test messages in both integrated and nonintegrated mode.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Test all required TUIs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Create and print faxes, if fax service is installed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Test system outcalling using Subscriber Options.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove any test subscribers.</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Complete the installation:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Register the MSS in ART:</td>
<td>130</td>
<td>Required for all systems that Avaya supports.</td>
</tr>
<tr>
<td>● With the modem active, register the MSS to program the product ID and remote access automatically.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Update MAS RAS information, if needed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set up logins and remote access on the MSS:</td>
<td>130</td>
<td>Do as required.</td>
</tr>
<tr>
<td>● Administer required logins on the MSS to grant access to authorized parties.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Complete PPP server configuration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specify Modem Dialout, SNMP, or Internet alarm origination on the MSS, and test alarm origination.</td>
<td>133</td>
<td>Procedure varies for Modem Dialout, SNMP, or Internet alarming.</td>
</tr>
<tr>
<td>Do an attended backup on each MAS.</td>
<td>139</td>
<td>Do this on each MAS.</td>
</tr>
<tr>
<td>Do an attended backup on the MSS. Discuss unattended backup methods with the customer.</td>
<td>141</td>
<td>Leave DVD backup in place.</td>
</tr>
</tbody>
</table>

Table page 5 of 6
<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Install additional software or client applications if required.</td>
<td>142</td>
<td>Do if required.</td>
</tr>
<tr>
<td></td>
<td>Copy the most current DCT data file to each MAS.</td>
<td>138</td>
<td>When done, delete the data file from your storage device.</td>
</tr>
<tr>
<td></td>
<td>Hand off system to the customer for further administration.</td>
<td>143</td>
<td></td>
</tr>
</tbody>
</table>

Table page 6 of 6
Modular Messaging on a customer-provided MAS installation checklist

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.

<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td><strong>Complete preinstallation requirements:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>If Avaya is to maintain the system, preregister the system in ART. The registration process produces product IDs for the servers and IP addresses for remote access.</td>
<td></td>
<td>You can obtain all required information for the MAS in advance.</td>
</tr>
<tr>
<td>✓</td>
<td>Assemble and review the required documentation.</td>
<td>9</td>
<td>Web access required.</td>
</tr>
<tr>
<td>✓</td>
<td>Download required software updates, including the latest version of the DCT executable file (MMDCT.exe), Pre-upgrade and Backup Verification Tool and client software.</td>
<td>10</td>
<td>Web access required.</td>
</tr>
<tr>
<td>✓</td>
<td>Obtain the DCT data file (*.mmdct) for this site.</td>
<td>9</td>
<td>Local procedures vary</td>
</tr>
<tr>
<td>✓</td>
<td>Review security considerations.</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Obtain the required anti-virus software for the MAS if required.</td>
<td>14</td>
<td>Customer obtains the software.</td>
</tr>
<tr>
<td>✓</td>
<td>Gather the necessary test equipment and tools.</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Arrange for initial switch and LAN administration. Register MAS corporate computer names on the DNS if required. <strong>Note:</strong> Avaya is not responsible for the installation, administration, or test of communications between customer computers and the LAN.</td>
<td>15</td>
<td>See LAN administrator.</td>
</tr>
<tr>
<td>✓</td>
<td>Verify that the switch or PBX is administered.</td>
<td>15</td>
<td>See switch administrator.</td>
</tr>
<tr>
<td>✓</td>
<td>Review preinstallation site requirements such as environmental requirements, weight and space considerations, power and grounding requirements.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td>✓</td>
<td>Review hardware requirements.</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
</tbody>
</table>

Table page 1 of 5
## Modular Messaging on a customer-provided MAS installation checklist

<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prepare for corporate Windows domain installs— do the tasks in this section only if the MM system is joining the corporate Windows domain:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create user accounts in the corporate Windows domain. This step is done by the corporate domain admin.</td>
<td>17</td>
<td>Review requirements in Chapters 4 and 5.</td>
</tr>
<tr>
<td></td>
<td>Create computer accounts in the corporate Windows domain. This step is done by the corporate domain admin.</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Install any required hardware:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Install the Dialogic port boards.</td>
<td></td>
<td>For details, see the Dialogic documentation. IP H.323 or IP SIP switch integrations skip this step.</td>
</tr>
<tr>
<td></td>
<td>Connect the MAS port boards to the switch or PBX.</td>
<td></td>
<td>Do as required.</td>
</tr>
<tr>
<td></td>
<td>Complete the hardware installation by installing and configuring each MAS modem.</td>
<td></td>
<td>Do as required.</td>
</tr>
<tr>
<td></td>
<td>Do initial MSS administration:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Log on to the MSS.</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adjust the monitor settings if needed.</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Start the MSS configuration using a DCT data file</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the time and date</td>
<td>31</td>
<td>Must do manually before configuring an MAS</td>
</tr>
<tr>
<td></td>
<td>Configure a new CPE MAS:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: The customer domain administrator may be required to perform these tasks. To configure Avaya-provided MAS, see Configure the MAS—repeat this section for each MAS and the Supplementary server: on page 256.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Complete the configuration pre-requisites.</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Install Microsoft Windows 2003 R2 with SP2 operating system, if not previously installed.</td>
<td>87</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the computer name</td>
<td>87</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Run recommended disk checks</td>
<td>87</td>
<td></td>
</tr>
</tbody>
</table>

Table page 2 of 5
## Modular Messaging on a customer-provided MAS installation checklist

<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Install and enable required MS Windows services.</td>
<td>88</td>
<td>Requires Microsoft Windows media.</td>
</tr>
<tr>
<td></td>
<td>Install required Microsoft Windows updates and security patches</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Install Microsoft Windows 2003 SP2</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adjust system values</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify if the Network Connections are set up correctly.</td>
<td>92</td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td></td>
<td>Verify network adapters and bindings</td>
<td>93</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change the Power Management settings</td>
<td>93</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Install and launch the Modular Messaging Configuration Wizard.</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Complete the CPE MAS configuration:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter the RAS IP addresses</td>
<td>98</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set logging location</td>
<td>98</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Install anti-virus software</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure and test the port boards if required, including:</td>
<td>99</td>
<td>Configuration notes required. Skip this step for IP-type or automatically configured integrations.</td>
</tr>
<tr>
<td></td>
<td>● For analog boards, create or use a valid tone file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Configure each port board.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Test incoming and outgoing calls on each board.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specify the preferred language for administration.</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify that Modular Messaging service is started.</td>
<td>55</td>
<td></td>
</tr>
</tbody>
</table>

Table page 3 of 5
<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Use the Voice Mail System Configuration (VMSC) program to configure required domain-wide settings on MAS#1:  
  ● TUI and administration access settings  
  ● PBX parameters using the configuration notes  
  ● Serviceability settings for Modem Dialout, SNMP, or Internet alarming  
  For MultiSite specific configuration, see Voice Mail System Configuration section in Avaya Modular Messaging MAS Administration Guide. For information on MultiSite concepts and requirements, see Avaya Modular Messaging MultiSite Feature Description Guide. | 56   | Do these tasks on MAS#1.  
  Configuration notes required for PBX settings.                                                                                                           |
| Use the VMSC to get the VMD ID needed for the license and submit the request. Install the license file after delivery and set up TTS sessions for each MAS.                                                                               | 60   | Local procedures vary.                                                                           |
| Configure the Call Me, Notify Me, MWI, Audit, Fax, language or TTS, and offline access (do OLA only on the last server). Reconfigure any of these services that are not enabled or are enabled on the wrong server. | 64   | Set up the features and services that are required on each MAS or on the Supplementary server. |
| Configure specific parameters for this MAS, including:  
  ● Modem Dialout alarming, if used  
  ● Port boards and switch integration settings using the configuration notes.                                                                                                                                   | 74   | Do for each MAS.  
  Configuration notes required.                                                                                                                             |
| Restart the messaging service.  
  ● Verify that the services that are not required on this MAS are disabled. Do not start all MM services until this is done.  
  ● Verify that all MM services required on this server are started and set to automatic.                                                                                                               | 77   | Ensure that the correct services are enabled on each MAS.                                           |
| Restart service on all MASs in the VMD as a final step.                                                                                                                                                         |      | Do after last MAS.                                                                              |

**Complete initial MSS administration:**

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch the monitor to show the MSS.</td>
<td>22</td>
</tr>
<tr>
<td>Continue the MSS configuration using a DCT data file</td>
<td>102</td>
</tr>
<tr>
<td>Configure the MSS modem</td>
<td>115</td>
</tr>
<tr>
<td>Install any software updates, if needed</td>
<td>116</td>
</tr>
</tbody>
</table>

**Do acceptance tests and run backups:**

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Table page 4 of 5</td>
<td></td>
</tr>
</tbody>
</table>

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
## Modular Messaging on a customer-provided MAS installation checklist

<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Add a test subscriber on MSS for each TUI used at this site.</td>
<td>114</td>
<td>MM Aria is the default.</td>
</tr>
<tr>
<td></td>
<td>Set up monitoring tools:</td>
<td>118</td>
<td>Optional, used for troubleshooting.</td>
</tr>
<tr>
<td></td>
<td>● Operational History Viewer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Port monitor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Do acceptance tests:</td>
<td>120</td>
<td>Do on CPE MAS that is set up to handle calls.</td>
</tr>
<tr>
<td></td>
<td>● Create and send a call-answer message.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Retrieve test messages in integrated mode.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Create and send a test message in nonintegrated mode.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Test the outcalling capability.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Create and print a fax message</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Run additional tests.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove the test subscribers from MSS.</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Back up the system.</td>
<td>139</td>
<td>Use local procedures.</td>
</tr>
<tr>
<td></td>
<td>Set up the system to perform regularly, scheduled backups.</td>
<td>141</td>
<td>Use local procedures.</td>
</tr>
<tr>
<td></td>
<td>Turn the system over to the customer.</td>
<td>143</td>
<td>Be sure to give the customer an updated DCT data file.</td>
</tr>
</tbody>
</table>
Modular Messaging Release 5.0 upgrade and migration checklists

This section of the Appendix provides two check lists that can be used to:

- Upgrade to Modular Messaging Release 5.0 from Release 3.x or Release 4.0 that runs on S3500 hardware.
- Migrate from Release 2.0, Release 3.x or Release 4.0 to Modular Messaging Release 5.0 system that runs on S8730-family server.

After you complete a task, make a checkmark in the ✔ column.

⚠️ Important:

- If you are moving the Modular Messaging system to the corporate Windows domain, first complete the entire upgrade (all releases), and then go to Moving the MM system to the corporate Windows domain checklist on page 274.
- If you must add a new MAS to an existing Modular Messaging system, first complete the entire upgrade for release that you planned. You must then install the new MAS using the new installation checklist.

The following check lists are covered in the subsequent sections:

- Modular Messaging Release 3.x or 4.0 on S3500-family server upgrade checklist on page 266.
- Modular Messaging Release 5.0 system migration checklist on page 269.
Module Messaging Release 3.x or 4.0 on S3500-family server upgrade checklist

Use this checklist to upgrade Module Messaging Release 3.x or Release 5.0 on S3500 server. As you complete a task, make a check mark in the "✓" column.

<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Plan for the upgrade:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| ✓ | Assemble and review the required software and the documentation:  
  ● Installation and Upgrade Guide  
  ● Data Collection Tool (DCT)  
  ● Pre-Upgrade and Backup Verification Tool  
  ● System Checklists  
  ● Planning for upgrade of clients in addition to the Module Messaging system (such as Outlook Client, Web Client, Speech Access, Web Subscriber Options). | 9 | Web access required (see http://support.avaya.com > Modular Messaging > Installation, Migrations, Upgrades and Configurations) |
| ✓ | Manually check the following items:  
  ● No errors or warnings are shown on the system  
  ● Resolve major and minor alarms  
  ● Backups are done  
  ● Private IP addresses are in the correct range  
  ● Private IP addresses on the same subnet  
  ● Corporate IP addresses on the same subnet  
  - Make sure that the private IP and corporate IP addresses do not use the same subnet  
  ● Private name of the MSS is MSS1  
  ● Corporate name is not mss1.b.c  
  ● List of non-standard installations (need help from the MMIUS team for a complete list)  
  ● Correct errors  
  ● Use the time estimates to set customer expectations for the time required to complete the upgrade. | | |
| | | 155 | |
| ✓ | Review product functionality with the customer:  
  ● Customer noticeable differences for MM 3.x/4.0  
  ● Known issues (see Product Support Notices)  
  ● Rollout plan for new features  
  ● Security concerns. | | |
| | | | |
| ✓ | Coordinate with MMTAC:  
  ● Submit DCT for approval  
  ● Provide implementation schedule for Tiered Support. | | |
| | | | |
| | **Prepare for the upgrade:** | | |
| | | Table page 1 of 3 | |
## Modular Messaging Release 3.x or 4.0 on S3500-family server upgrade checklist

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download any required Avaya software updates, including the Outlook Client.</td>
<td>10</td>
<td>Web access required.</td>
</tr>
<tr>
<td>Verify the key settings on the MSS and MAS, such as switch integration, port board settings, and domain information:</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>● Verify if the MM system is at required Patch and SP level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Verify the MSS has recommended RFU installed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Record information for non-default port groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Record RAS IP addresses for each MAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Back up Caller Applications files on separate computer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Record associations for Caller Application (will be needed for re-association later)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Record SNMP trap destination and community details from the <strong>Serviceability - Voice Mail Domain</strong> window</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain and review the configuration notes for any changes.</td>
<td>150</td>
<td>Web access required.</td>
</tr>
<tr>
<td>Use the Pre-Upgrade tool (PUBVT):</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>● Download and run the Pre-upgrade tool</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Correct errors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Use the time estimates to set the customer expectations for the time required to complete the upgrade.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Be prepared to delay the upgrade if everything is not in order. It is better to delay and do it right than to go ahead and get it wrong!**

**Prepare for the upgrade on the MAS:**

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch the monitor to show the correct server.</td>
<td>149</td>
</tr>
<tr>
<td>Verify that all Modular Messaging servers and services are running.</td>
<td></td>
</tr>
<tr>
<td>Run the Pre-Upgrade Tool</td>
<td>153</td>
</tr>
<tr>
<td>Analyze every MAS and create a Data Collection Tool (DCT) file:</td>
<td>156</td>
</tr>
<tr>
<td>● Download the current version of the DCT</td>
<td></td>
</tr>
<tr>
<td>● Run the DCT in &quot;analyze&quot; mode on each MAS</td>
<td></td>
</tr>
<tr>
<td>● Verify the DCT file.</td>
<td></td>
</tr>
<tr>
<td>Busy out ports on each MAS.</td>
<td>159</td>
</tr>
<tr>
<td>Check for any spooled messages.</td>
<td>160</td>
</tr>
<tr>
<td>Back up each MAS.</td>
<td>161</td>
</tr>
</tbody>
</table>

Table page 2 of 3
## Modular Messaging Release 3.x or 4.0 on S3500-family server upgrade checklist

<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Back up the MSS.</td>
<td>162</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Run Backup Verification tool</td>
<td>164</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perform the upgrade:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Load the updated software on the MSS.</td>
<td>166</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade the MSS.</td>
<td>166</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Log off all remote logins.</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade overnight</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade RealSpeak only if you are upgrading from Release 3.x.</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade Dialogic drivers on the MAS.</td>
<td>171</td>
<td>For any MAS that already has drivers installed.</td>
</tr>
<tr>
<td></td>
<td>Upgrade the MAS software. Includes software (Windows updates, service pack(s), and patches) and configuration of Fax and Audit services.</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Complete the upgrade:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Complete the upgrades.</td>
<td>176</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Convert the Supplementary server to run a 0 port MAS:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Optional: Convert the Supplementary server to run a 0 port MAS on the Supplementary server.</td>
<td>178</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change the switch integration:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Optional: Change the switch integration as appropriate depending on the type of switch integration involved.</td>
<td>181</td>
<td></td>
</tr>
</tbody>
</table>
Modular Messaging Release 5.0 system migration checklist

Use this checklist to migrate Modular Messaging to S3730 server. As you complete a task, make a check mark in the "✔️" column.

Modular Messaging Release 5.0 system migration checklist:
Planning for the migration

<table>
<thead>
<tr>
<th>✔️</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Plan for the migration:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>Complete a project plan for the upgrade, including</td>
<td>9</td>
<td>Local procedures vary.</td>
</tr>
<tr>
<td></td>
<td>● Project schedule</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Definition of roles</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Assignment of resources (staff)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Internal kickoff meeting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Planning for upgrade of clients in addition to the MM system (such as Outlook Client, Web Client, Speech Access).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>Assemble and review the required software and documentation required for migration:</td>
<td>9 and 202</td>
<td>Web access required (see <a href="http://support.avaya.com">http://support.avaya.com</a> &gt; Modular Messaging &gt; Installation, Migrations, Upgrades and Configurations)</td>
</tr>
<tr>
<td></td>
<td>● Installation and Upgrade Guide</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Data Collection Tool (DCT)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Pre-Upgrade and Backup Verification Tool</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● System Checklists</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Web Client Installation and Upgrades.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>Assemble and review relevant Product Support Notices (PSNs) and Product Correction Notices (PCNs).</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>If a design is required, verify that it was received from ATAC. Review design output with the implementation team. Design review is required for the following upgrades:</td>
<td>149</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Replacement of all S3400/3500 servers (MSS and MAS) with S8730 servers</td>
<td>205</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Addition of a new MAS to the configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Removal of an MAS from the configuration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>Switch the monitor to show the correct server.</td>
<td>149</td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>Use the Pre-Upgrade tool (PUBVT):</td>
<td>205</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Download and run the Pre-upgrade tool</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Correct errors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Use the time estimates to set customer expectations for the time required to complete the upgrade.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table page 1 of 3
## Installation and upgrade checklists

### Modular Messaging Release 5.0 system migration checklist:
### Planning for the migration

<table>
<thead>
<tr>
<th>✓ Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Analyze every MAS and Supplementary server, and create a Data Collection Tool (DCT) file:  
  - Download the current version of the DCT  
  - Run the DCT in "analyze" mode on each MAS  
  - Verify the DCT data file. | 206  |              |
| Review product functionality with the customer:  
  - TUI difference document(s), as needed  
  - Customer noticeable differences  
  - Known issues (see Product Support Notices)  
  - Rollout plan for new features  
  - Security concerns. | 206  |              |
| Verify key settings on the MSS and MAS, such as switch integration, port board settings, and domain information:  
  - Record information for non-default port groups  
  - Record RAS IP addresses for each MAS  
  - Back up Caller Applications files on separate computer  
  - Record associations for Caller Application (will be needed for re-association later).  
  - Record SNMP trap destination and community details from the Serviceability - Voice Mail Domain window | 150  |              |
| Review the upgrade with the entire implementation team:  
  - Review output from the Pre-Upgrade tool, Data Collection Tool, and Checklists  
  - Discuss the upgrade process, known issues, questions about documentation, customer expectations and concerns, time required for upgrade, and back-out plan. |      |              |
| Coordinate with MMTAC:  
  - Submit DCT for approval  
  - Provide implementation schedule for Tiered Support. |      |              |

### Prepare for the migration:

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download any required Avaya software updates.</td>
<td>10</td>
<td>Web access required.</td>
</tr>
<tr>
<td>Obtain and review the configuration notes for any changes.</td>
<td>11</td>
<td>Web access required.</td>
</tr>
</tbody>
</table>
Modular Messaging Release 5.0 system migration checklist:
Planning for the migration

<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Process and set up new hardware (replacement S8730s for MSS and/or MAS, S8730 for additional MAS):</td>
<td></td>
<td>See Installing the Avaya S8730 Server for Modular Messaging guide.</td>
</tr>
<tr>
<td></td>
<td>● Unpack equipment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Review inventory checklist</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Pre-register new hardware</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Rack and stack only (power off, no software installation).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Be prepared to delay the upgrade if everything is not in order. It is better to delay and do it right than to go ahead and get it wrong!</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prepare for the migration on the MAS:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Busy out ports on MAS</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check the spooled messages</td>
<td>211</td>
<td>Do not use old backups.</td>
</tr>
<tr>
<td></td>
<td>Do a fresh, attended backup on each MAS</td>
<td>212</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Backup the data from the MSS</td>
<td>212</td>
<td></td>
</tr>
</tbody>
</table>

Table page 3 of 3

Modular Messaging Release 5.0 system migration checklist:
Implementing the upgrade

<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Migrate the MSS:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Run the Backup Verification tool</td>
<td>213</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore data on the MSS.</td>
<td>213</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Migrate each MAS and the Supplementary server, if present:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Start the MAS migration.</td>
<td>217</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Install and administer anti-virus software.</td>
<td>220</td>
<td>Local procedures vary.</td>
</tr>
<tr>
<td></td>
<td>Install the latest Avaya-approved updates for Microsoft Windows: system updates and security patches.</td>
<td>220</td>
<td>Local procedures vary.</td>
</tr>
<tr>
<td></td>
<td>Reapply the remote access settings to each MAS.</td>
<td>221</td>
<td></td>
</tr>
</tbody>
</table>

Table page 1 of 3

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
## Modular Messaging Release 5.0 system migration checklist: Implementing the upgrade

<table>
<thead>
<tr>
<th>✓</th>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify and update settings in the VMSC, including:</td>
<td>222</td>
<td>Verifies settings for switch integration and configured features as required.</td>
</tr>
<tr>
<td></td>
<td>● Update Security permissions for system administration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Verify license settings and TTS sessions per MAS.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Verify port board and telephony interface settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Set up additional port groups, if required at this site.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Optional</strong> - Create offline message store on the server that hosts offline messages.</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restart messaging services.</td>
<td>228</td>
<td>Do after last MAS.</td>
</tr>
<tr>
<td></td>
<td>● Verify that all services not required on this MAS are disabled. Do not start all MM services until this is done.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Verify that all MM services required on this server are started and set to Automatic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Complete VMSC setup (enter MAS product IDs, configure Fax and Audit services, verify services)</td>
<td>230</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Complete MSS administration:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify the MAS host information for each MAS.</td>
<td>232</td>
<td>Logins and passwords changed on the MAS because of the W2003 server so make sure you do this step.</td>
</tr>
<tr>
<td></td>
<td>Place the MSS in the private Windows domain.</td>
<td>233</td>
<td>Do this once per upgrade.</td>
</tr>
<tr>
<td></td>
<td><strong>Restore data on each MAS:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stop all Modular Messaging services.</td>
<td>235</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore data on each MAS from most current backup.</td>
<td>236</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore Caller Applications on MAS#1.</td>
<td>238</td>
<td>Do if Caller Applications are used on the system.</td>
</tr>
<tr>
<td></td>
<td>Restart messaging services and verify correct services are started.</td>
<td>239</td>
<td>Make sure MM service connector is started.</td>
</tr>
<tr>
<td></td>
<td>Install any Avaya software updates.</td>
<td>240</td>
<td>You must install software updates if they’re available.</td>
</tr>
<tr>
<td></td>
<td>Repeat data restoration for each MAS.</td>
<td>236</td>
<td></td>
</tr>
</tbody>
</table>
Modular Messaging Release 5.0 system migration checklist: Implementing the upgrade

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do messaging acceptance tests, including:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Create and receive test messages in both integrated and nonintegrated mode.</td>
<td>241</td>
<td>Tests vary per MAS and system setup.</td>
</tr>
<tr>
<td>● Test all supported TUIs as required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Create and print faxes, if fax service is installed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Test system outcalling using Subscriber Options.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continue migration for additional MASs and Supplementary server, if present.</td>
<td>217</td>
<td></td>
</tr>
</tbody>
</table>

**Complete the system migration:**

- Analyze the system using the DCT file. 242
- Do an attended backup on each MAS. 242
- Remove old MAS backup files from the MSS. 244 Do this for each MAS.
- Do an attended backup on the MSS. 245
- **Optional:** Add new S8730-family servers to this system 341 Use the new system installation checklist.
- Update and turn over DCT data file. 247 When done, erase the data file from your storage device.

**Update or install new client software:**

- Update or install any additional software required on each MAS, such as: 248
  - Modular Messaging Web Subscriber Options
  - Avaya Modular Messaging Notes Client
  - Avaya Modular Messaging Outlook Client
  - Avaya Modular Messaging Outlook Restricted
  - Mailbox Manager
- **Optional:** Reduce the number of MASs in your VMD. 249
- **Optional:** Change switch integration. 251
- **Optional:** Move to the corporate Windows domain after migration. 252

Table page 3 of 3
## Moving the MM system to the corporate Windows domain checklist

<table>
<thead>
<tr>
<th>Preparing for the move to the corporate Windows domain:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete the upgrade or migration to Release 5.0.</td>
</tr>
<tr>
<td>Create user accounts in the corporate Windows domain.</td>
</tr>
<tr>
<td>Create computer accounts in the corporate Windows domain.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Move servers to the corporate Windows domain:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare the system before moving subsequent servers.</td>
</tr>
<tr>
<td>Move subsequent servers.</td>
</tr>
<tr>
<td>Move the MSS to the corporate Windows domain.</td>
</tr>
<tr>
<td>Move MAS#1 to the corporate Windows domain.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Complete the move to the corporate Windows domain:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete the move to the corporate Windows domain.</td>
</tr>
</tbody>
</table>
Appendix B: 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 the voice mail system on page 53.

This section contains the following topics:

- When to configure port boards on page 276
- Configuring port boards on page 277
- Testing the port boards on page 287
When to configure port boards

In Release 5.0, 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.

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)
Supported port boards

All MASs support a maximum of two port boards each. Table 8 lists supported Dialogic port boards for S8730-family servers.

Table 8: Supported MAS port boards: S8730 hardware

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Maximum Ports per MAS</th>
<th>Port boards</th>
<th>Maximum cards per MAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analog</td>
<td>24</td>
<td>Dialogic D/120JCT-LS-EW 12-port board</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Dialogic D/41JCT-LS-EW 4-port board</td>
<td>2</td>
</tr>
<tr>
<td>Digital Set Emulation</td>
<td>16</td>
<td>Dialogic D/82JCT-EW</td>
<td>2</td>
</tr>
<tr>
<td>E1-QSIG</td>
<td>60</td>
<td>Dialogic D/600JCT-1E1-120-EW</td>
<td>2</td>
</tr>
<tr>
<td>T1-QSIG</td>
<td>46</td>
<td>Dialogic D/480JCT-1T1-EW</td>
<td>2</td>
</tr>
<tr>
<td>H.323 integration</td>
<td>30</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SIP¹</td>
<td>48</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

1. SIP and H.323 transmit voice as IP packets over the LAN cards. Therefore, does not need separate port boards.

The Dialogic documents provide details required to install and connect the port boards; see Downloading user documentation on page 12.

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 to get the most recent configuration notes, see Downloading configuration notes on page 11.
Configuring and testing port boards

⚠️ **CAUTION:**

You can only install this system 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. You must complete the port board configuration as described in Configuring port boards and switch integration on page 75.

Continue based on the type of port boards installed in this MAS:

- Configuring T1-QSIG or E1-QSIG boards on page 279
- Configuring set emulation boards on page 280
- Configuring analog port boards on page 282

⚠️ **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, get the appropriate maintenance information for this Modular Messaging system; see Downloading user documentation on page 12:

- For S8730-family servers, get Avaya Modular Messaging S8730-Family Hardware Maintenance and Additions.
- For S3500-family servers, get Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions.

For information on placing and numbering the Dialogic port boards, see Installing the Avaya S8730 Server for Modular Messaging 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
- Dialogic D/480JCT-1T1- EW
- Dialogic D/600JCT-1E1
- Dialogic D/600JCT-2E1
- Dialogic D/600JCT-1E1- 120- EW

The maximum number of port boards per MAS varies, depending on the server hardware. For more information, see Supported port boards on page 277.

To configure either of these 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.**

      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 Intel Dialogic services are stopped. All boards should show a red icon.

4. If the board icon shows an X, the board is disabled. To enable it, right-click the board and select **Enable device(s).**

5. Under Configured Devices, double-click the name of the first Dialogic board, such as #0.

6. 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

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Configuring and testing port boards

- For T1-QSIG: select μ-Law (mu-Law) for the United States and Japan
  e. Click the Misc tab.
  f. For the FirmwareFile parameter, verify that the value is default.
  g. Select the FirmwareFile2 parameter. Type spfax.fwl in the Value field, which is editable.
  h. Click the Country tab and select the Country parameter.
  i. On the pull-down list of values, always use United States for either type of board.
  j. Click OK to close the window.

7. Repeat Steps 5 and 6 for any other installed Dialogic boards, such as #1.

8. 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.

9. 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 5 through 9 as needed.


11. Continue with Testing the port boards on page 287.

---

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 277.

Note:
Avaya supports the non-universal Dialogic D/82JCT-EW board for upgrades only.

To configure digital set emulation boards:

1. Click Start > Programs > Dialogic System Release > Configuration Manager - DCM.
   The 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 **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 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 reboot the MAS before you start the Dialogic drivers. Close the DCM and reboot the system now. When the reboot 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.

---

**Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.**
Configuring and testing port boards

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.


10. Continue with Testing the port boards on page 287.

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
   ● 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 277.

To configure either of these analog boards:

1. Click Start > Programs > Dialogic System Release > Configuration Manager - DCM.
   The 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 5.0, 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 5.0:

a. Under Configured Devices, double-click the name of the Dialogic board, such as #0.

b. In the 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 Dialogic Product Configuration Manager window.

b. Wait 30 seconds for all the Dialogic processes to completely stop.

c. Reopen the 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.

Note:
If the drivers fail to start, complete Steps 6 through 16. You must then completely power down and power up the MAS. After the server boots, continue with Testing the port boards on page 287.

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.
Configuring and testing port boards

⚠️ **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 D: Creating a new tone file on page 315.

7. In the **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 C:\Avaya_Support\Tone_Files.
      
      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 13 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 287.

11. Close the Dialogic product Configuration Manager window.
    Continue with Testing the port boards on page 287.

12. In the Dialogic product Configuration Manager - Properties window:
    a. Click the Files tab.
    b. Select the TSFFileName parameter, if it is not already selected.
    c. Locate the prerecorded TSF file for this PBX or switch:
       1. Click the ... button to browse. In the Look In field, navigate to C:\Avaya_Support\Tone_Files.
       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:

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.

13. 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.

14. Repeat Steps 6 through 13 for any other installed Dialogic boards, such as #1. Verify that the settings are correct, and set any values if needed.

15. 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 287.

17. Continue with Testing the port boards on page 287.
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, turn off and then turn on the server for the port board to work. 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. Double-click the Monitor icon on the desktop.
   b. Click 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 Stop.

2. 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. Click **Start > Programs > Avaya Modular Messaging > Dialogic Line Tester**.

   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 individual port extensions.

   b. Check the **Status** column.
      
      - Verify that each port shows **Received call** followed by **Connected**.
      - For different status conditions, see **Table 9**.

   The system should answer each connected call with a standard welcome message.
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.
   c. Click **Dial Number**.
   d. When the dialed extension rings, answer the call and hang up.
   e. Select the next port number, and click **Dial Number** again.
   f. Repeat Steps d and e until all ports are tested.

5. After testing is complete, close the **Dialogic Line Test Application** window.

---

### Table 9: Status messages for Dialogic Line Test

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Highlight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel starting…</td>
<td>The channel is being started.</td>
<td>Normal</td>
</tr>
<tr>
<td>Channels idle…</td>
<td>The channel is idle.</td>
<td>Normal</td>
</tr>
<tr>
<td>Waiting for call…</td>
<td>The channel is waiting for an incoming call.</td>
<td>Normal</td>
</tr>
<tr>
<td>Received call…</td>
<td>An incoming call is being processed.</td>
<td>Normal</td>
</tr>
<tr>
<td>Dialling number…</td>
<td>A number is being dialed to make an outgoing call.</td>
<td>Normal</td>
</tr>
<tr>
<td>Resetting…</td>
<td>The user reset the channel.</td>
<td>Normal</td>
</tr>
<tr>
<td>Line Busy.</td>
<td>An outgoing call was made, but a busy tone was detected.</td>
<td>Normal</td>
</tr>
<tr>
<td>No Answer.</td>
<td>An outgoing call was made, but the call was not answered.</td>
<td>Normal</td>
</tr>
<tr>
<td>Connected.</td>
<td>An incoming or outgoing call was answered, so the call is now connected.</td>
<td>Normal</td>
</tr>
<tr>
<td>Call was disconnected.</td>
<td>An incoming or outgoing call was disconnected.</td>
<td>Normal</td>
</tr>
<tr>
<td>Error.</td>
<td>A general error with the channel occurred.</td>
<td>Error</td>
</tr>
<tr>
<td>Error. No Dial tone detected.</td>
<td>An outgoing call was made, but no dial tone was detected before dialing.</td>
<td>Error</td>
</tr>
</tbody>
</table>

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Configuring and testing port boards

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. After port board testing is complete, continue as appropriate:
   ● For new installations, continue with Configuring MAS port boards on page 52.
   ● For migrations, continue with Updating settings in the VMSC on page 222.
Appendix C: Installing Dialogic port boards in a customer-provided MAS

This chapter describes how to install Dialogic port boards and their drivers in a customer-provided equipment (CPE) server, also called a customer-provided MAS. A customer might have several servers that support Avaya Modular Messaging software and services.

- One to five 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 in a customer-provided equipment (CPE) server that is to handle calls.

Continue with [Performing initial MSS administration](#) on page 21 if:

- you are using Avaya-provided hardware, For detailed procedures, see *Installing the Avaya S8730 Server for Modular Messaging* guide or *Maintaining the Avaya S8730 Server for Modular Messaging* 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.

⚠️ **CAUTION:**

Avaya does not support Brooktrout port boards for Modular Messaging systems that run Release 5.0 software. Install only the currently supported Dialogic port boards in a CPE server.

Avaya recommends that you connect a modem to each server to support remote dial in.

**Note:**

Before you can do the tasks described in this section, verify that all preinstallation requirements were met as described in [Preinstallation requirements](#) on page 7.

Topics in this chapter include:

- [Supported MAS port boards](#) on page 293
- [Installing MAS port boards](#) on page 295
- [Connecting MAS port boards to the switch](#) on page 307
- [Completing the hardware installation](#) on page 308
Installing Dialogic port boards in a customer-provided MAS

- Configuring port boards on page 308
- Testing the port boards on page 313
Supported MAS port boards

Table 10 lists the Dialogic port boards that Avaya supports for all new installations that use customer-provided equipment (CPE) 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 10: Supported MAS port boards for customer-provided servers

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Ports per MAS</th>
<th>Port boards</th>
<th>Maximum Number</th>
<th>Dialog files on documentation media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analog</td>
<td>12 - 24</td>
<td>Dialogic D/120JCT-LS 12-port board</td>
<td>2</td>
<td>D/120JCT-LS (PDF)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dialogic D/120JCT-LS- EW 12-port board</td>
<td>2</td>
<td>D/120JCT-LS -EW (PDF)</td>
</tr>
<tr>
<td></td>
<td>4 - 8</td>
<td>Dialogic D/120JCT-LS- EWEU (Europe) 12-port board</td>
<td>2</td>
<td>D/41JCT-LS (PDF)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dialogic D/41JCT-LS 4-port board</td>
<td></td>
<td>D/41JCT-LS- EW (PDF)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dialogic D/41JCT-LS- EW 4-port board</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dialogic D/41JCT-LS- EWEU (Europe) 4-port board</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Digital Set Emulation</td>
<td>8 - 16</td>
<td>Dialogic D/82JCT-U-PCI-UNIV</td>
<td>2</td>
<td>D/82JCT-U PCI Univ (PDF)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dialogic D/82JCT-EW</td>
<td></td>
<td>D/82JCT-EW (PDF)</td>
</tr>
<tr>
<td>E1-QSIG</td>
<td>30 - 60</td>
<td>Dialogic D/600JCT-1E1 1 or D/600JCT-2E1</td>
<td>2</td>
<td>D/600JCT-1E1 or D/600JCT-2E1 (PDF)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dialogic D/600JCT-1E1- 120- EW</td>
<td></td>
<td>D/600JCT-1E1-120-EW</td>
</tr>
<tr>
<td>T1-QSIG</td>
<td>23 - 46</td>
<td>Dialogic D/480JCT-1T1 1 or D/480JCT-1T1- EW</td>
<td>2</td>
<td>D/480JCT-1T1 (PDF)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dialogic D/480JCT-1T1-EW</td>
<td></td>
<td>D/480JCT-1T1-EW (PDF)</td>
</tr>
</tbody>
</table>

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 shipped after mid-2005 have only a single connector. Both types of QSIG boards operate identically.

Note:
To support the capacities shown in Table 10, the minimum CPE server hardware specifications must match the specifications for the S3500-family MAS. For more information, see the Avaya Modular Messaging Concepts and Planning Guide.

a. The Dialogic documents provide details about installing and connecting the port boards. The documents are available on the Avaya Modular Messaging Documentation media or from the www.avaya.com/support Web site. For instructions on how to obtain the documents, see Downloading required software and documentation on page 9. For the latest version of the Dialogic guides, see the Quick Install Cards Search Tool on the Dialogic Web site.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Installing Dialogic port boards in a customer-provided MAS

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 equipment (CPE) 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 10: Supported MAS port boards for customer-provided servers on page 293.

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 media.

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 10: Supported MAS port boards for customer-provided servers on page 293.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Installing Dialogic port boards in a customer-provided MAS

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 10: Supported MAS port boards for customer-provided servers on page 293.

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 297
   - D/480JCT-1T1-EW and D/600JCT-E1-120-EW QSIG board settings on page 297
   - D/82JCT-U PCI Univ set emulation board settings on page 298
   - D/82JCT-U EW set emulation board settings on page 299
   - D/120JCT-LS 12-port analog board settings on page 300
   - D/120JCT-LS-EW port analog board settings on page 300
   - D/41JCT-LS 4-port analog board settings on page 301
   - D/41JCT-LS-EW analog board settings on page 303
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 11.

   Table 11: D/480JCT-1T1 and D/600JCT-1E1 or D/600JCT-2E1 QSIG board ID settings

<table>
<thead>
<tr>
<th>Card number</th>
<th>Board ID number</th>
<th>PCI slot number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

   Note:

   Do not set the Computer Telephony (CT) bus for bus termination.

2. Continue with Installing the port boards on page 305.

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 11.

   Table 12: D/480JCT-1T1-EW and D/600JCT-E1-120-EW QSIG board ID settings

<table>
<thead>
<tr>
<th>Board ID number</th>
<th>PCI slot number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

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 13.

Table 13: D/82JCT-U set emulation board settings for CT bus termination

<table>
<thead>
<tr>
<th>Number of cards</th>
<th>P8 jumper</th>
<th>CT bus termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OFF</td>
<td>Do not terminate bus.</td>
</tr>
</tbody>
</table>
| 2               | Card 1: ON pins 1 and 2
                   | Card 2: ON pins 1 and 2             | Terminate bus on both boards.       |

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.

2. Continue with Installing the port boards on page 305.
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 13.

Table 14: D/82JCT-U set emulation board settings for CT bus termination

<table>
<thead>
<tr>
<th>Number of cards</th>
<th>P8 jumper</th>
<th>CT bus termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OFF</td>
<td>Do not terminate bus.</td>
</tr>
<tr>
<td>2</td>
<td>Card 1: ON pins 1 and 2 Card 2: ON pins 1 and 2</td>
<td>Terminate bus on both boards.</td>
</tr>
</tbody>
</table>

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

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 15.

   Table 15: D/120JCT-LS 12-port analog board ID settings

<table>
<thead>
<tr>
<th>Card number</th>
<th>Board ID number</th>
<th>PCI slot number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

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

   ![Figure 3: D/120JCT-LS analog board setting for on-hook switch](image)

3. Continue with Installing the port boards on page 305.

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.
Installing MAS port boards

The Dialogic port boards usually are placed in the PCI slots starting from the right side of the cabinet, see Table 16.

Table 16: D/120JCT-LS-EW port analog board ID settings

<table>
<thead>
<tr>
<th>Board ID number</th>
<th>PCI slot number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

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

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 17.

Table 17: D/41JCT-LS 4-port analog board ID settings

<table>
<thead>
<tr>
<th>Card number</th>
<th>Board ID number</th>
<th>PCI slot number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

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

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Installing Dialogic port boards in a customer-provided MAS

hook-switch state. See Figure 5: D/41JCT-LS analog board setting for on-hook switch on page 302.

Figure 5: D/41JCT-LS analog board setting for on-hook switch

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 18.

Table 18: D/41JCT-LS analog board settings for CT bus termination

<table>
<thead>
<tr>
<th>Number of cards</th>
<th>JP2 jumper</th>
<th>CT bus termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OFF</td>
<td>Do not terminate bus.</td>
</tr>
<tr>
<td>2</td>
<td>Card 1: ON pins 1 and 2 Card 2: ON pins 1 and 2</td>
<td>Terminate bus on both boards.</td>
</tr>
</tbody>
</table>

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
**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 19.

   **Table 19: D/41JCT-LS 4-port analog board ID settings**

<table>
<thead>
<tr>
<th>Board ID number</th>
<th>PCI slot number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

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 303.

---

**Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.**
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 20**.

**Table 20: D/41JCT-LS-EW analog board settings for CT bus termination**

<table>
<thead>
<tr>
<th>Number of cards</th>
<th>JP2 jumper</th>
<th>CT bus termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OFF</td>
<td>Do not terminate bus.</td>
</tr>
</tbody>
</table>
| 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.

3. Replace and tighten the retaining screw for the port board.
4. Repeat Steps 1 through 3 to install any additional port boards.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Installing Dialogic port boards in a customer-provided MAS

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.
     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

The Dialogic port boards require their own drivers and software for board configuration. To complete the hardware installation on a customer-provided equipment (CPE) server, 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 95.

Configuring port boards

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 the voice mail system on page 53.

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 to get the most recent configuration notes, see Downloading configuration notes on page 11.

⚠️ CAUTION:

You can only install this system 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. You must complete the port board configuration as described in Configuring port boards and switch integration on page 75.

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 311
- Configuring analog port boards on page 312
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, get the appropriate maintenance information for this Modular Messaging system; see Downloading user documentation on page 12:

- For S8730-family servers, get *Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions.*

- For S3500-family servers, get "Circuit card replacement."

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Installing Dialogic port boards in a customer-provided MAS

Configuring T1-QSIG or E1-QSIG boards

Any of the following QSIG port boards might be installed in an MAS:

- Dialogic D/480JCT-1T1
- Dialogic D/480JCT-1T1- EW
- Dialogic D/600JCT-1E1
- Dialogic D/600JCT-2E1
- Dialogic D/600JCT-1E1- 120- EW

The maximum number of port boards per MAS varies, depending on the server hardware. For more information, see Configuring port boards on page 308.

To configure either of these QSIG boards:

1. Click Start > Programs > Dialogic System Release > Configuration Manager - DCM.

   The 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.

      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.

4. If the board icon shows an X, the board is disabled. To enable it, right-click the board and select Enable device(s).

5. Under Configured Devices, double-click the name of the first Dialogic board, such as #0.

6. In the 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
Configuring port boards

- For T1-QSIG: select \( \mu\text{-Law} \) (mu-Law) for the United States and Japan.
  
e. Click the Misc tab.
  
f. For the FirmwareFile parameter, verify that the value is default.
  
g. Select the FirmwareFile2 parameter. Type spfax.fwl in the Value field, which is editable.
  
h. Click the Country tab and select the Country parameter.
  
i. On the pull-down list of values, always use United States for either type of board.
  
j. Click OK to close the window.

7. Repeat Steps 5 and 6 for any other installed Dialogic boards, such as #1.

8. 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.

9. 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 5 through 9 as needed.


11. Continue with Testing the port boards on page 313.

---

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 Configuring port boards on page 308.

Configure the port boards as outlined in Configuring set emulation boards on page 280. You may install Dialogic D/82JCT-EW board in an MAS.

Note:

Avaya supports the non-universal Dialogic D/82JCT-U-PCI-UNIV board for upgrades only.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
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
- 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 Configuring port boards on page 308.

Configure the analog port boards as outlined in Configuring analog port boards on page 282.
Testing the port boards

Test all port boards and channels to verify that port boards can send and receive calls using the procedures outlined in Testing the port boards on page 287.

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, turn off and then turn on the server again. The power cycle corrects the port board problems.
Installing Dialogic port boards in a customer-provided MAS
Appendix D: 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 282.

°C A N U T I O N:

Use the configuration notes for the PBX or switch integration to administer the port boards. For instructions to get the configuration notes, see Downloading required software and documentation on page 9. 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 316.

● **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 319.

**Note:**

If only one line is connected to the Dialogic port board, you must use Manual Learning.

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

This section describes:

- Running the PBXpert wizard on page 316
- Consolidating and saving the TSF file on page 318
- Using the new TSF in Dialogic Configuration Manager on page 319

Running the PBXpert wizard

The PBXpert wizard guides you to learn the tones used by the PBX and save 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.
   
   The Intel Dialogic product Configuration Manager window must be open
   
   a. 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 have change any of the settings.
   - 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 continue.
   - If the line test fails:
     - Click **OK**. Close this window.
     - Click **Back**, adjust the settings, and try the test again.
Creating a new tone file

8. On the Learning Tones screen, click **Next** to start learning tones automatically.
   The Learn Tones window opens.

   **Note:**
   You can click **Cancel** anytime 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 continue.
   - 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 continue.
    - 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.

   **Note:**
   If you use the default DATA directory, the system will not save 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 282 and complete board configuration and testing.

Learning tones manually

This section describes:

- Running PBXpert on page 319
- Adding a new tone set on page 320
- Learning tone definitions on page 321
- Testing the tone set on page 321
- Consolidating and saving the TSF file on page 322
- Using the new TSF in Dialogic Configuration Manager on page 322

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.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Creating a new tone file

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, 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 the 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** anytime 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 continue.
   - 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 282 and complete board configuration and testing.
Appendix E: Updating Modular Messaging software

You might 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.

Topics in this appendix include:

- Getting software updates from the Web on page 324
- Installing software updates on each MAS on page 325
- Installing software updates on the MSS on page 328

Considerations for applying updates include:

- You can apply multiple patches to a system.
- You can apply multiple updates to Modular Messaging components.
- If you apply a Service Pack, the program automatically uninstalls all previously applied patches and Service Packs.
Getting software updates from the Web

Get the latest Avaya software updates from the Web.

To get any Avaya software updates for the system:

1. Use a computer that can access the Internet.
3. Click the link to FIND DOCUMENTATION and TECHNICAL INFORMATION by PRODUCT NAME.
4. Under M, click Modular Messaging.
5. On the Modular Messaging page, select Release 5.0 from the drop-down list.
6. Click Downloads.
7. Download the files needed to update the Modular Messaging system.

Note:
Ensure that you download both the software files and any instructions required to install the Service Pack or software patch.

8. Copy the downloaded files to a storage device.
9. Use the appropriate tools on your computer to extract the files into an appropriate directory. The files are often in a compressed form, such as a zip file.
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. For more information, see Switching the monitor to show the correct server on page 149.

2. Insert the storage device into the server.

3. Copy the software update files to the MAS:
   a. Open Windows Explorer.
   b. Navigate to the appropriate directory on the storage device.
   c. Right-click the software update file that you downloaded in Getting software updates from the Web on page 324. For example, file MAS300100.exe. Select Copy.
   d. Navigate to the C:\Avaya_Support directory.
   e. Right-click in a blank area in the right pane, and select Paste.
   f. Verify that the correct file is pasted in the C:\Avaya_Support directory.
   g. If you have downloaded more than one file, repeat Steps c through f to copy the software files and the update instructions to the MAS.

4. Remove the storage device from the server:

5. Repeat Steps 1 through 4 for each MAS in the system.

6. Open and review the installation instructions for this specific software update.

   Note:
   A software update might contain updates for the MAS only, the MSS only, or both servers. To complete the update, use the instructions as a guideline, altering the instructions to fit the update situation.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Installing the updates on each MAS

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

To install the Avaya software updates on the MAS:

1. Log on as the Domain Administrator or Service Pack Installer account so that you can copy the updates to the MSS.

2. Double-click the software update file for this MAS, such as `MAS300100.exe`.

   The program unpacks the file and then runs the Modular Messaging Installation Wizard.

3. In the Modular Messaging Installation Wizard window:
   a. Select all applicable patches for this system.

   Note:
   You must install updates for the MSS once for each software update. If you want to update a subsequent MAS and have already installed the MSS update, ensure that you cleared the **Message Storage Server Update** check box.

   b. Click **Install**.

   Note:
   If the **Install** button is not active, you do not need to apply these software updates to the system. Continue with Step 6.

4. If you are installing a Service Pack (SP), an Installation Wizard - Update Warning window opens. The window displays the patches and Service Packs that the program must remove before the update can continue. Click **Continue**.

5. After you click **Install**, monitor the software update progress:
   a. In the Services window, the Modular Messaging Installation Wizard stops all appropriate Modular Messaging and related services.
   b. Windows Installer then installs all relevant software updates on the MAS.
   c. If any updates apply to the MSS, the program transfers the appropriate files to the MSS.
   d. If prompted, reboot the system.

6. To verify the software updates installed on the MAS:
   a. Logon to the MAS.
   b. Select **Start > Programs > Avaya Modular Messaging**.
   c. Click the **About Modular Messaging** tab.

      The About tab shows the version of MM installed
d. Click the **Patches** tab.

You can see the Service Packs and Patches installed on the system.

7. After installation and verification is complete, close all open windows.
Installing software updates on the MSS

⚠️ Important:
Read the Release notes for each software update for specific information. The following sections only contain general instructions for installing updates on the MSS.

To continue the software update procedure, you must install any available updates on the MSS.

1. Toggle the port on the KVM switch to have the monitor show the MSS. For more information, see Switching the monitor to show the correct server on page 149.

2. Log on to the MSS server as craft using the appropriate password.

3. From the Software Management menu, click Software Update > Service Pack.

⚠️ CAUTION:
If you see a warning about the backup that is incomplete within the last 2 hours, click Cancel. Save the server data before you continue. For more information, see Setting up and running a backup on the MSS on page 141.

4. The system might report that the installed version is current. In this case, the MSS already has the most recent software updates installed. Do not take any further action. Log off the server.

5. If an update is present, click Proceed with Service Pack Installation.
   The system reports that a reboot is required.

6. Click Proceed with Installation.
   The system installs the updates on the MSS.

7. Verify that the installation completed successfully.

8. Click Reboot servername.

9. At the reboot warning message, click OK to continue.
   The system displays status messages as the server shuts down the messaging software. The shutdown process can take several minutes.
Appendix F: Moving Modular Messaging services

You must distribute the Modular Messaging services across all installed MASs, and the Supplementary server if present. This practice balances the load on the system for optimum performance.

Use the procedures described in this section to redistribute Modular Messaging services:

- after you add a new MAS or a Supplementary server to the system
- to optimize performance the system in service.

This appendix describes how to move the Modular Messaging services across MASs, and the Supplementary server if present.

This section includes the following topics:

- Disabling Modular Messaging services you plan to move on page 330
- Moving Modular Messaging services among servers on page 331
- Enabling the services on the correct server on page 338

See Avaya Modular Messaging Concepts and Planning Guide guide on recommendations for the distribution of Modular Messaging services and tools among MASs that use S8730-family hardware.
Disabling Modular Messaging services you plan to move

Before you move any Modular Messaging services, you must disable the service 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 on multiple servers that is supposed to run on only one.

Use the following steps to disable services that are currently running on a server:

1. Log on to each server that you intend to move Modular Messaging services from.
2. Double-click the Monitor icon on the desktop or from command prompt, run services.msc.
3. Click Services (Local) in the left pane, if the service is not already selected.
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:
   1. MM Call Me—must be on the same server with the Mailbox Monitor Server
   2. MM Mailbox Monitor—must be on the same server with Call Me and MWI
   3. MM MWI—must be on the same server with the Mailbox Monitor Server
   4. MM Fax Sender Service —enable on a server with voice ports that support Fax calls
   5. MM Tracing Service—enable on only one server in the VMD
6. Refresh the screen to verify that all MM services that you plan to move are Disabled.
Moving Modular Messaging services among servers

Moving the Modular Messaging services involves the following steps:

1. Log on to the MAS or Supplementary server to which you intend to move Modular Messaging services.

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 332
   - Moving MM Fax Sender service on page 334
   - Moving Audit server on page 336
   - Moving Tracing service on page 336
Moving Modular Messaging services

Moving Call Me, MWI, and Mailbox Monitor

You must enable Call Me, Message Waiting Indicator (MWI), and Mailbox Monitor services only once in the voice mail domain. All three services must be enabled on the same server.

Updating the Call Me configuration

Use the following steps to change the parameters for Call Me configuration:

1. In the voice mail domain, such as vmdom, double-click Call Me.
2. Click the General tab.
3. In the MAS Call Me server field, specify the server on which to enable the Call Me service. If the field is blank:
   a. Click the ... next to the field.
   b. In the Select Computer window, enter the name of the MAS you chose as your MAS Call Me server.
   c. Click Check Names.
   d. Click OK to accept the MAS name and close the window.

Note:
As Call Me and Message Waiting Indicator (MWI) services use the Mailbox Monitor, you must enable both services on the same server.
Updating the MWI configuration

Use the following steps to change the Message Waiting Indicator (MWI) configuration parameters:

1. In the voice mail domain, such as vmdom, double-click **Message Waiting Indicator**.
2. In the Message Waiting Indicator - Voice Mail Domain window, click the **General** tab.
3. In the **MAS MWI server** field, specify the server on which the MWI Service is enabled. If the field is blank:
   a. Click the ... button next to the field.
   b. In the **Select Computer** window, enter the name of the MAS you chose as your MAS Call Me server.
   c. Click **Check Names**.
   d. Click **OK** to accept the MAS name and close the window.
   e. Click **OK** to close this window.
4. For the **Limit requests** and **Maximum requests per minute** fields, use the values specified in the configuration notes for your PBX integration type.
5. In the **Messaging Application Servers that support MWI** box, list all MASs that have a port group set up to support MWI. Use the following steps to add a server name:
   a. Double-click inside the top of the big list box, or click the **Add** 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, such as **MYMAS2**.
   d. Repeat Steps b and c to add any other MASs that support MWI, such as **MYMAS1**.
   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 proceed to each additional MAS if needed.

6. Click **OK** to close this window.
7. Log on to the MSS server as **craft** using the appropriate password.
8. Click **Messaging Administration >Trusted Servers**.
   The system opens the **Manage Trusted Servers** page.
9. Select and edit the VVSTS entry:
   a. Change the IP address to the IP address of the new MWI server.
   b. Click **Save**.
   c. Click **OK**.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
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 ports. IP H.323 switch integration does not support fax service.

Use the following steps to move MM Fax Sender service:

Enable MM Fax Sender service on the MAS that will now host MM Fax Sender service:

1. Run \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 no longer hosts the 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. Clear the Share this printer checkbox.
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. The system opens the Printers and Faxes window.
3. Right-click the Fax and select Properties.
4. Click the Security tab.
5. Add the Network Service user and assign that user Print, Manage Printers, and Manage Documents permissions.
6. Click the Sharing tab.
7. Select the Share this printer checkbox. Leave the share name as Fax.
8. Select the List in the directory check box.
9. Click Additional Drivers. The system opens the Additional Drivers dialog box.
10. Select the client operating systems installed on the network that can use the Fax Printer. The Fax Printer drivers are downloaded when you first connect the system to the Fax Printer.
11. Click OK.
12. Click the **Security** tab.

13. Verify that **Everyone** is assigned Fax permissions on the share.

**Note:**

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 330
2. Open the **Monitor** window on the MAS that will now host MM Fax Sender or from the command prompt, run `services.msc`.
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.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
4. On the "restart" window, click OK.

Moving Audit server

Audit service is installed on each MAS in the VMD. Complete the following steps to change the MAS that acts as an MM Audit Server:

1. In the Voice Mail System Configuration window, in the voice mail domain, double-click Auditing.
2. In the Auditing - Voice Mail Domain window, on the General tab, select the Enable Auditing checkbox.
3. In the Audit server field, specify the server that acts as the MM Audit server. If the field is blank:
   a. Click the ... button next to the field.
   b. In the Select Computer window, enter the name of the MAS you chose as your MAS Call Me server.
   c. Click Check Names.
   d. Click OK to accept the MAS name and close the window.
   e. Click OK to close this window.
4. In the Database server field, enter the name of the server where the database resides or click browse (....) and select the server.
5. Click OK to close this window.

Moving Tracing service

To move the Tracing Service to a different server:

1. Log in to the MAS to which you intend to move the Tracing Service.
2. Access the Voice Mail System Configuration program. Click Start > Programs > Avaya Modular Messaging > Voice Mail System Configuration.
3. Under the voice mail domain, such as vmdom, double-click Tracing System.
   The system may display a warning that the current Home Message Application Server is not valid. You must then click OK.
4. 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.
5. Click OK to close this window.
6. 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. 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 them 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 or from command prompt, run services.msc.
   b. Click Services (Local) in the left pane, if the item is not already selected.
   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.
Enabling the services on the correct server

To enable the appropriate Modular Messaging services:

1. In the **Monitor** window or from command prompt, run **services.msc**.
2. Click **Services (Local)** in the left pane, if the item is not already selected.
3. In the right pane, scroll down to the list of Modular Messaging services. These services start with the abbreviation **MM**.

**CAUTION:**
You must enable some Modular Messaging services only once in a voice mail domain, or serious problems will occur. For more information, see Table 5.

4. 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 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 services**

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.

---

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Moving Modular Messaging services

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 338. 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.
Appendix G: Adding an MAS or a Supplementary server to an existing system

This appendix describes how to add an Avaya Messaging Application Server (MAS) or a Supplementary server to an existing Modular Messaging system that is already in service.

All servers must meet the requirements listed in the *Avaya Modular Messaging Concepts and Planning Guide*. You can download the document using the instructions provided in *Downloading user documentation* on page 12.

Topics in this chapter include:

- **MAS configuration prerequisites** on page 342
- **Adding a new server to a system in service** on page 343
- **Configuring the new server** on page 349
MAS configuration prerequisites

To set up a server, you need:

- All required hardware installed. For more information about how to install the server, see *Installing the Avaya S8730 Server for Modular Messaging* guide.

- The following software from the Avaya Support Web site at [http://www.avaya.com/support](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 9.
  - Avaya software updates that are required to bring the Modular Messaging software up to date after an installation. Download the software to a storage device.
  - The latest copy of the Data Collection Tool and DCT data file. Download the `MMDCT.exe` file from the Avaya support Web site to a storage device. If a DCT file was created for this installation, download `MMDCT.exe` to the same storage device as the DCT data file.

- Microsoft Windows Service Pack 2, if not previously installed for customer-provided server only.
Adding a new server to a system in service

The section describes how to add an MAS or a Supplementary server to a Modular Messaging system that is already in service.

⚠️ CAUTION:
You cannot add a new server to a Modular Messaging system during an upgrade to Release 5.0. You can replace the server hardware with a new model, but you cannot change the number of servers until after the upgrade is complete. Follow the instructions outlined in Migrating to Modular Messaging Release 5.0 on S8730-family server on page 201 to migrate to S8730. If you have not upgraded the system to Release 5.0, complete the upgrade as instructed in Upgrading to Modular Messaging Release 5.0 on S3500-family server on page 145 and proceed with instructions in this section to add a new server.
Adding an MAS or a Supplementary server to an existing system

Installing the new MAS or a Supplementary server

You can install one or more servers after an initial upgrade or new installation. You can add one or more of the following servers, one at a time:

- One or more Messaging Application Server (MAS)s, up to the limit allowed by the system.
- A Supplementary server, if one is not already present in the system.
- A combination of MASs and a Supplementary server.

To install a new Avaya Messaging Application Server (MAS) or a Supplementary server:

1. Install the S8730-family MAS or Supplementary server hardware. For more information, see Installing the Avaya S8730 Server for Modular Messaging guide.

   Tip:
   Use the new server installation checklist for this configuration of Modular Messaging system as a guide to avoid missing steps. See Installation and upgrade checklists on page 253.

2. Before you configure the new servers, prepare the message store to recognize the new servers. Continue with Preparing the MSS for the new servers on page 345.
Preparing the MSS for the new servers

If you add one or more MASs or a Supplementary server to a system, you must configure the MSS so that it can identify the new server.

Adding a new trusted server on the MSS

You must add a trusted server for each MAS or Supplementary server in the voice mail domain.

⚠️ CAUTION:
Use the DCT file to enter the correct values for the trusted servers.

Use the following steps to set up the new server as a trusted server on the MSS:

1. Toggle the port on the KVM switch to have the monitor show the MSS.
2. Log on to the MSS as craft.
4. Click Add a New Trusted Server and enter the following information:
   a. In the Trusted Server Name field, enter the customer-specified NetBIOS name for this MAS, such as mymas1.
   b. In the Password field, enter the LDAP password to be used for all MASs in this Modular Messaging system. Type the password again in the Confirm Password field.
   c. In the Machine Name / IP Address field, enter the correct private IP address for this MAS as listed in Private IP addresses for each MAS by IP address range on page 34.
   ⚠️ CAUTION:
   You must use the same private IP address range on the MSS that you will use on each MAS. Ensure that the private network settings in the Modular Messaging Data Collection Tool match with the settings on this page.
   d. In the Special Type field, click Messaging Application Server from the drop-down list, to add a trusted server for an MAS or a Supplementary server.
      The Special Type selection populates the other fields with the required values.
5. After you verify or update the information, click Save.
6. At the confirmation message, click OK.
7. If you are adding an MAS or a Supplementary server, repeat the process for each MAS and Supplementary server.
Using the DCT to analyze the current configuration

Before you can configure the new server, you must ensure that the DCT data file for the Avaya Modular Messaging system is complete and current. To do this, you must collect information from each MAS in the system, including the Supplementary server, if present. The data file allows the Avaya Modular Messaging Configuration wizard to configure the new server automatically.

Use the following steps to collect data from each MAS and the Supplementary server, if present:

1. Verify that the Modular Messaging system works normally and that the correct services run on each MAS and Supplementary server.
2. Ensure that you have a current copy of the DCT file to use as a guide.
3. Switch the monitor to show the server to analyze.

⚠️ CAUTION:
Do not stop or disable any Modular Messaging services that you plan to move at this stage. All currently installed services must run normally for the DCT analysis to be successful.

4. Verify that the required messaging services on this server are running:
   a. Double-click the Monitor icon on the desktop.
   b. Click Services (Local) in the left pane, if the item is not already selected.
   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 Started for each messaging service that belongs on this server. For a list of required services, see DCT data file.

   Note:
   If service is not started for a required messaging service, right-click the specific MM service and select Start. The system starts the messaging service.

5. Insert a storage device that contains the DCT program, MMDCT.exe into the MAS.
   a. Copy the MMDCT.exe to the C:\Program Files\Avaya Modular Messaging\Install\MISCM directory.
   b. Double-click the C:\Program Files\Avaya Modular Messaging\Install\MISCM\MMDCT.exe file. The system opens Avaya Modular Messaging Data Collection Tool window.

6. Update the most current data file for the system:
   a. In the Select the DCT Configuration to use dialog box, select Analyze existing system. Click OK.
   b. When the program prompts you to use an existing DCT file, click Yes.
Adding a new server to a system in service

c. In the Open window, click the drop-down list next to Look in.

d. Navigate to the location of the most current DCT data file.
   - For MAS#1, navigate to the MAS directory
     C:\Program Files\Avaya Modular Messaging\Install\MISCM\cfg.
   - For a subsequent MAS or the Supplementary server, navigate to the most current data file on the storage device, Removable disc (E:).

e. Double-click the current data file for this site, such as sitefile.mmdct.
   The system opens the MM System Analysis window.

❗ CAUTION:
For a multiple-MAS system, you must open the same data file that you saved on the previous MAS. Otherwise, the data from that server is lost. Do not enter the data for subsequent servers manually! Use the DCT to analyze each server in turn. The tool collects some data that does not appear on the DCT screens.

7. Click the appropriate number for the server. In the MAS Information is being collected from field, click the appropriate number for the server:
   - For MAS#1, select First MAS (#1).
   - For a subsequent MAS or a Supplementary server, select the appropriate number for this server, such as Second MAS (#2).

   Note:
   Analyze the MASs in numeric order, first to last.

8. Click Start.
   The system displays the process of data collection. When the analysis is complete, the system displays "information has been successfully collected" message and then opens Avaya Modular Messaging Data Collection Tool window.

9. Verify the data on each screen. For more information, see Avaya Modular Messaging Data Collection Tool Online Help.

10. Click Complete.

11. Save the 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. Enter the name of the data file in the File name field, such as sitefile.
   d. Leave the file type set as MM DCT Files (*.mmdct).
   e. Click Save.
   f. If the system prompts you to replace an existing data file, click Yes.
   The system closes the Avaya Modular Messaging Data Collection Tool window.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Adding an MAS or a Supplementary server to an existing system

12. Safely remove the storage device from the server to prevent damage to the data file:
   a. Double-click the icon on the task bar to **Safely Remove Hardware**.
   b. Follow the prompts to safely remove the hardware.
   c. Close all open windows.

13. Continue as appropriate:
   ● If the system has additional MASs or a Supplementary server, return to Step 3.
   ● After all servers in the system are analyzed, continue with [Configuring the new server](#) on page 349.
Configuring the new server

Use the updated DCT data file and the Avaya Modular Messaging Configuration wizard to configure the new server.

Running the configuration wizard

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 complete the following:
      ● For an Avaya-provided server, select MSS with Avaya MAS servers.
      ● For a customer-provided server, select MSS with customer’s MAS servers. This selection tells the system that you want to install customer-provided equipment.
   c. Under MM servers, Click Voice Mail Domain. On the system Voice Mail Domain screen complete the following:

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Adding an MAS or a Supplementary server to an existing system

1. Update the **Number of MASs in the VMD**. Include all additional servers that you are installing, whether they are MASs or a Supplementary server.

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 ensure 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 **Full Computer Name** field and **IP address** field for each MAS and Supplementary 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. 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** checkbox. Leave all other services set as they are.

      ● For a Supplementary server, do **not** select the **Message Application** checkbox. Do not select any other services. Leave the **MAS** column for the new server blank.

   h. 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**.
Configuring the new server

Note:
When the server configuration is complete, copy this updated DCT data file to the other servers in the system, so all servers have the same data. You must also send a copy of the current data file to the technical support group using the procedures appropriate for this site. For more information, see Completing the Add New MAS or Supplementary server on page 352.

7. 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.

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

8. 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 reboots.

9. After the reboot 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 a new S8730-family server, the product key sticker is located on the right hand edge of the server chassis.
   c. Click Next.

The Avaya Modular Messaging Configuration Wizard displays the configuration status. The server reboots several times, but you do not need to log on manually. The entire process takes about 25 minutes.

10. When the server configuration is complete, the progress bar stretches across the screen and the Next button becomes active. Click Next.


-------------------------------------------------------------------------------------------------------------------
Completing new server configuration

Use the following steps to complete the new server configuration and setup:

1. Configure the new MAS or a Supplementary server and test that the server works. Use the procedures described in Configuring the Avaya MAS on page 41. For a customer-provided server, use the procedure Configuring a customer-provided MAS on page 85.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
2. Proceed with Moving Modular Messaging services on page 329.

⚠️ **CAUTION:**
Before you activate the Modular Messaging services on a new server, complete all other VMSC administration required for this server. For more information on VMSC configuration see Configuring the voice mail system on page 53.

---

### Completing the Add New MAS or Supplementary server

Use the following steps to complete adding new MAS or a Supplementary server:

1. Verify basic server operation and do the appropriate acceptance tests as instructed in Running acceptance tests on page 120.

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 to analyze all the servers in the system again. For more information, see Using the DCT to analyze the current configuration on page 346.

3. To ensure that all servers have the most current information, copy the updated DCT data file from the USB storage device to each server:
   a. Using Windows Explorer, copy the updated DCT data file to the MAS directory `C:\Program Files\Avaya Modular Messaging\Install\MISCM\cfg`

   **Tip:**
   Rename the existing data file in this directory before you copy the new one, as a backup. For example, rename the existing data file `sitefile-old.mmdct`.

   b. Remove the storage device from the server to prevent damage to the data file:
      1. Double-click the icon on the task bar to **Safety Remove Hardware**.
      2. Follow the prompts to safely remove the storage device.

   c. Insert the storage device into the next MAS or Supplementary server.
   d. Repeat Steps a through c for each MAS and Supplementary server in the system.

4. Update and turn over DCT data file.
   a. Send a copy of the most current DCT data file to the appropriate technical support group.
   b. Erase the copy of the DCT data file from your USB storage device.
Appendix H: Reloading MAS and MSS software

This appendix describes how to reload the operating system and the application software on an Avaya Messaging Application Server (MAS) (or an Avaya-provided supplementary server) and Message Storage Server (MSS).

Topics in this appendix include:

- Loading new MAS software on page 353
- Loading new MSS software on page 357

Loading new MAS software

Complete the procedures described in this section to reload Modular Messaging software to the Avaya Messaging Application Server (MAS) or Avaya-provided supplementary server.

Switching the monitor to show the correct server

1. If the server is not on, turn on the server.
2. Verify that the monitor shows the correct server.
   - For a 2-port KVM switch, the MSS is connected to one of the computer port.
   - For an 8-port Belkin KVM switch, the MSS usually is connected to the first computer port on the switch. The port is labeled VGA 01.
3. If the monitor displays a different server, toggle the port to show the correct MAS.
   - To have a 2-port Belkin KVM switch show a different server:
     a. 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 1 for port 1.
   - To have an 8-port Belkin KVM switch show a different server:
     a. Gently press Scroll Lock twice within 2 seconds.
     b. Select the server to display using 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 using the keyboard. For example, type 1 for port 1.
4. For complete user and troubleshooting instructions on KVM switch, see the KVM switch documentation.

---

### Loading the new software

To load the new software on the MAS or the supplementary server:

1. Insert the following disks into the DVD drive:
   - For S8730 server, insert the 'Avaya Modular Messaging R5.0 MAS for Avaya Store Model S8730 Boot' disk.
   - For S3500 server, insert the 'Avaya Modular Messaging R5.0 MAS for Avaya Store Model S3500 Boot' disk.

   Wait for green LED on the drive to turn off.

2. Close the DVD drive tray.

3. Press Ctrl+Alt+Delete to reboot the system.
   a. In the Windows Security window, click Shut Down...
   b. In the Shut Down Windows window, select Restart. Click OK.

4. When the computer starts to boot, the system displays a warning that the hard drive contents will be overwritten.
   a. Press any key to continue. The system displays a message to confirm that the hard disk drive will be overwritten.
   b. Press any key to continue.

   The MAS starts to copy the disk image to the hard disk.

5. After the software is copied, the program prompts you to remove the media before the system reboots.
   a. Remove the disk from the drive and close the drive tray.
   b. Press Ctrl+Alt+Delete to continue.

   The system reboots, and runs a Windows Setup program.

6. If you have Intel Dialogic cards installed, the system opens a Security Alert window that prompts you to install the driver for the Dialogic card. Click Yes.

7. If you have connected a modem, a Hardware Installation window opens. Click Yes to continue the installation.

8. A Windows Setup wizard runs. To complete the wizard:
   a. On the Welcome screen, click Next.
   b. On the License Agreement screen, select I accept this agreement. Click Next.
   c. On the Your Product Key screen, type the Windows product key for the server.
Note:
Each Windows computer has a unique product key for the Windows 2003 R2 operating system. Enter the number exactly as shown.

- For a new S8730-family server, the product key sticker is located on the right hand side of the server chassis.
- For an S3500-family server, which uses the Windows 2003 operating system, the product key sticker is located inside the empty drive tray on the lower-left of the server chassis.

d. Click Next.
The server automatically reboots.

Note:
On servers that use the latest motherboard, you might see System Event Log Full when the system boots. You can ignore this error message.

Activating Microsoft Windows

You must activate the Microsoft Windows operating system when you reload the operating system. You must activate the Windows operating system before you restart the MAS.

To activate the Microsoft Windows operating system:

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 you installed the Modular Messaging system.
   b. Call the appropriate telephone number shown on the screen.
   c. Follow the voice prompts or the directions from the customer service representative to provide the unique installation ID shown on the screen.
   d. Enter the confirmation ID that the automated system or the customer service representative gives you.
   e. Click Next.
4. On the confirmation screen, click Finish.
Preparing the server to boot

You must load all required information and activate the operating system before you activate the server configuration program:

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.

2. You must activate the Microsoft Windows operating system before you restart the server. For the Windows activation procedure, see Activating Microsoft Windows on page 355.

3. To complete the software reload, double-click the MM_Setup icon on the desktop.
   a. On the MM_Setup window, when the system prompts you, insert the 'Modular Messaging R5.0 MAS Application DVD 1 of 2' disk into the MAS, and press any key to continue.
   b. Follow instructions that appear.
   c. When the system prompts you, remove the disk from the MAS and press any key to continue.
      MM_Setup reports that the Modular Messaging configuration program will run after the server reboots.
   d. Press any key to continue.
      The computer stores the information and shuts down.

4. To bring the server into service, continue with the appropriate procedure:
   - For a new system installation, continue with the procedure, which has pointed you to this section.
   - For a hard disk drive repair or other system problem, continue with the maintenance procedure. For more information, see the appropriate document:
      - Maintaining the Avaya S8730 Server for Modular Messaging
      - Avaya Modular Messaging S3500-Family Hardware Maintenance and Additions
      - Avaya Modular Messaging MAS Catastrophic Disk Failure Recovery
Loading new MSS software

To copy new software to the MSS:

1. If the Message Storage Server (MSS) is not on, turn on the server.

2. Verify that the monitor is showing the MSS. For more information, see Switching the monitor to show the correct server on page 353.

3. Remove any storage device attached to the MSS, as this can interfere with the reload.

4. Insert the Modular Messaging R5.0 MSS OS disk into the MSS.

5. To reboot the system, do one of the tasks:
   - From the monitor:
     a. If the MSS displays the Web interface, click Logoff.
     b. From the localhost login: prompt, press Ctrl+Alt+Del.
   - From the MSS: Reset the server using the console on the front of the server.

Note:
You might see the System Event Log Full error message when the S3500 system boots. You can ignore this message. Modular Messaging does not use this log.

The computer starts to boot. The system then displays the following options:

2U Standard Availability (S3500)!standard2U <ENTER>.
HP Standard Availability (S8730)!standardHP <ENTER>.
2U High Availability (S3500)!high2U <ENTER>.
HP High Availability (S8730)!highHP <ENTER>.

6. At the boot: prompt, type the word for this model of MSS (the names are case sensitive, type exactly as shown) and then press Enter:
   - Type standard2U for an S3500-type MSS-S. This model has one horizontal disk drive.
   - Type standardHP for an S8730-type MSS-S. This model has two vertical disk drives, indicated by lit LEDs on the server drive bays.
   - Type high2U for an S3500-type MSS-H. This model has four horizontal disk drives, indicated by lit LEDs on the server drive bays.
   - Type highHP for an S8730-type MSS-H. This model has four vertical disk drives, indicated by lit LEDs on the server drive bays.

The system takes up to 20 minutes to copy the software. The system notifies when the software installation is complete.

7. Remove the Modular Messaging R5.0 MSS OS disk.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Important:
Do not leave the disk in the drive, or the system will boot from the disk. If you cannot eject the disk from the drive, start the system reboot, and then remove the disk. Click Reboot. The server reboots. To speed up the server reboot, press Escape to exit the splash screen. For S3500 server, you must press Space to skip the memory test.

8. On the Time Date Selection screen, set the time and date as follows:
   a. Use the up or down arrow keys to highlight the time zone.
   b. Press Tab key to move to the New Time section.
   c. Enter the current time in hh:mm (hours and minutes) format, based on a 24-hour clock.
   d. Press Tab key to move to the New Date section.
   e. Enter the current time in mm/dd/yy (month, day, and year) format, such as 12/03/09 for December 3, 2009.
   f. Press Tab key to move to the OK field. Press Enter.

9. When the system displays the localhost login prompt, type root and then press Enter.

10. Insert the Modular Messaging R5.0 MSS Application disk into the MSS.

   CAUTION:
   Wait for the drive light to stop flashing and go out before you continue.

11. At the prompt, type /etc/autoinstall and press Enter.

12. If the system prompts you to continue or quit, press Enter to continue.

13. The system prompts you to change several passwords.
   ● Enter the passwords that are provided for the following logins: root, craft, tsc, sroot, and craftppp.
   ● You can ignore any warnings, such as the passwords being too short.

   When the installation is complete, the system prompts you to remove the media from the drive.

14. Remove the Modular Messaging R5.0 MSS Application disk.

15. Press Enter to reboot the system.

   The system displays Press Enter to return to prompt..., press Enter.

16. At the localhost login prompt, log on to the MSS as craft.

   The server displays the Messaging Administration web interface.

17. To bring the server into service, continue with the appropriate procedure:
   ● For new system installations, continue with Performing initial MSS administration on page 21.
● For upgrades, continue with Checking the spool folder on each MAS on page 160.
● For a hard disk drive repair or other system problem, continue with the appropriate maintenance procedure. For more information about the procedures on maintenance and repair, see Maintaining the Avaya S8730 Server for Modular Messaging.
Reloading MAS and MSS software
Appendix I: 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 362
- Installing and configuring the AudioCodes gateway at switch location on page 363
- Continue configuring the AudioCodes gateway on page 366

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
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 from either a remote location or 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.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
Installing and configuring the 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 lose the changes made to IP Address, until you save the settings in step 4d described in Continue configuring the AudioCodes gateway on page 366.

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 customer’s 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 locally or from a location remote to the AudioCodes:

**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 362, 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 363.
   
   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.
   d. When the system prompts you, click OK.
7. 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.
8. 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.

9. Perform the acceptance tests on MASs using the AudioCodes gateway you have just configured as described in Performing acceptance tests for a new installation on page 117.
Installing and configuring the AudioCodes gateway
## Index

**A**

- about this book .................................................. 1
- acceptance tests ................................................... 117, 120, 121, 123, 124, 127, 241
- activating Microsoft Windows .................................. 355
- Add Local Subscriber page ........................................ 112, 113, 114
- add new MAS to the system ...................................... 83, 100, 247, 253
- Add Trusted Server page ........................................... 35, 36
- adding a server to a system ..................................... 341
- adding test subscribers .......................................... 114
- adding the MSS to the corporate Windows domain ........... 109
- adding the MSS to the private Windows domain ............... 108
- adding the MSS to the Windows domain (upgrade) .......... 223
- Address Range window .......................................... 221
- administering classes of service .............................. 110, 111
- administering special mailboxes on MSS ...................... 112
- Alarm Log page .................................................... 135
- alarm logs on MAS .................................................. 81
- Alarm Management page .......................................... 133
- alarm origination ................................................. 81, 133, 135
- alarming
  - disconnect modems for upgrades ............................ 159, 247
  - method to use .................................................. 58, 133
  - setup ............................................................. 58, 133
  - telephone number .............................................. 74
- analog boards
  - cabling .......................................................... 307
  - changing to QSIG .............................................. 181
  - configuring ..................................................... 282, 312
  - initial switch (PBX administration) ......................... 15
  - jumper settings ............................................... 300, 301, 303
  - supported boards ............................................. 277, 293
  - testing .......................................................... 287, 313
  - tone file ....................................................... 284, 285, 315, 316, 319
- announcement languages ........................................ 71, 158, 209
- anti-virus software
  - administering and using ..................................... 48
  - obtaining and installing .................................... 14, 48, 220
- ART
  - login account .................................................. 130
  - passwords ...................................................... 130
  - PPP logins ...................................................... 130, 132
  - product ID ..................................................... 63, 130, 133
  - RAS IP addresses ............................................. 50, 130
  - registering a server .......................................... 130
- ASA ................................................................. 37
- Assign/Change Password page ................................... 131
- assigning IP addresses ......................................... 27, 51, 221
- assistance (technical) .......................................... 5
- attended backup .................................................. 139, 141, 161, 162, 242, 245
- audio encoding .................................................. 56, 224
- Audit Service
  - Configuring .................................................... 67
- Avaya Automatic Registration Tool, see ART ................. 44, 136, 217, 276, 346, 349
- Avaya Modular Messaging Configuration wizard .............. 44, 136
- Avaya Modular Messaging Data Collection Tool, see DCT ... 44, 136
- Avaya Multi-site or Site Administration, see ASA ........... 110
- Avaya software updates, see software updates ............... 110

**B**

- backing up the system ......................................... 139, 141, 161, 162, 242, 245
- Backup page ...................................................... 141, 162, 245
- Backup Utility window .......................................... 236
- Backup Verification tool
  - installing ....................................................... 153
  - running ........................................................ 164, 213
- balance Modular Messaging services across servers ........ 329
- Brooktrout port boards ........................................ 291
- browser ........................................................... 47
- busyout ports .................................................... 159

**C**

- cabling
  - MAS port boards ............................................... 307
  - call answer test ............................................... 120
- Call Me - Voice Mail Domain window ........................... 65, 332
- Call Me Server .................................................. 65, 332
- Caller Applications
  - back up files .................................................. 156, 244
  - restoring ....................................................... 231, 238
- changes from last issue of book ................................ 2
- changing DSE or analog to QSIG ................................ 181
- changing DSE or QSIG to H.323 ................................ 183
- changing DSE or QSIG to SIP .................................. 184
- changing from DSE .............................................. 181
- changing H.323 to SIP .......................................... 187
- changing QSIG T1 to QSIG E1 .................................. 185
- checklist for installing new servers .......................... 344
- checklists
  - installing new system ....................................... 3, 21, 254
  - obtaining ....................................................... 11
  - upgrades ....................................................... 3, 4, 148, 202, 265
- class of service on MSS ......................................... 38, 110, 111
- client software packages
  - enabling permissions ......................................... 37
Index

- updating existing software .................................................. 142, 248
- comment on this book .......................................................... 6
- completing initial MSS administration ................................. 101
- computer accounts ................................................................. 18
- configuration notes ................................................................. 222
  * configuring VMSC ............................................................... 53, 75, 76
  * obtaining .............................................................................. 11
  * PBX integration settings ...................................................... 57
  * port boards .................................................... 277, 287, 308, 315
  * upgrades ............................................................................. 148, 156, 202
- Configure Network Addressing page ...................................... 27
- Configure Subscriber Management page ............................. 113
- Configure window ................................................................. 221
- configuring a new server .................................................... 349
- configuring domain-wide features ...................................... 54
- configuring MAS-specific parameters ................................. 75
- configuring Messaging Application Servers ......................... 74, 75, 76
- configuring port boards .......................................................... 52, 76, 222, 275, 277, 308
- Configuring System screen ..................................................... 45, 218, 351
- configuring the voice mail system ........................................ 53, 64, 74, 222
- Connect As window ............................................................... 236, 244
- contact information ............................................................... 6
- corporate administrator
  * creating computer accounts ............................................... 18
  * creating user accounts ..................................................... 17
  * preparing corporate Windows domain ................................ 16
- corporate LAN
  * settings on MSS ................................................................. 27
  * testing addresses with ping ................................................ 105, 107
- Corporate MM server networking details screen .................. 157, 208
- Corporate network details screen ........................................ 157, 208
- Corporate network screen .................................................... 157, 207
- corporate Windows domain ................................................... 138
- creating computer accounts ............................................... 18
- creating technical support accounts .................................... 17
- creating user accounts ....................................................... 17
- join (upgrade) ................................................................. 206
- MAS backup ....................................................................... 139
- moving to after upgrade ..................................................... 188
- placing MSS in domain ....................................................... 109
- preparing ............................................................................ 16
- remote access account ........................................................ 17, 19
- updating MAS host information ............................................ 106
- coverage path ................................................................... 15
- create the offline message share ......................................... 225
- creating a new tone file ........................................................ 315, 316, 319
- creating computer accounts ............................................... 18
- creating test messages .......................................................... 120, 123
- CT bus cable .................................................................... 306
- customer administration account ...................................... 158, 209
- Customer details screen ...................................................... 157, 207
- customer handoff ............................................................... 143
- customer responsibility for system security ......................... 13
- customer-provided equipment
- port boards ........................................................................ 293
- customer-provided MAS
  * adjusting system values .................................................... 90
  * installation checklist ....................................................... 260, 266, 269

D

- dadmin login ......................................................................... 131
- Data Collection Tool, see DCT
- date and time setup .............................................................. 31
- DCT
  * analyze servers ............................................................... 136, 346, 352
  * collecting data for upgrades ............................................ 156, 206
  * configuring a new server ................................................ 349
  * copy most recent data file to all servers ......................... 138
  * copying data file to all servers ....................................... 138, 352
  * correcting errors ............................................................ 157, 207
  * Data Collection Tool window ......................................... 44, 136, 137, 158, 209, 218, 346, 347, 349
  * data file ............................................................................. 3, 136, 143, 202, 247, 346, 352
  * final handoff of data file ............................................... 143, 247, 352
  * help .................................................................................. 9, 156, 207
  * saving data file ............................................................... 137, 158, 209, 347, 350
  * updating DCT data file ................................................... 137, 346
  * using existing data file ................................................... 44, 136, 347
  * deploying caller applications ......................................... 238
  * desktop client access ....................................................... 112, 114
  * specifying on MSS ............................................................ 38
- Dialogic Configuration Manager ......................................... 279, 280, 282, 310, 311, 312, 315
- Dialogic drivers ..................................................................... 306, 308
- Dialogic Line Test Application window ......................... 287, 286, 289
- disabling Modular Messaging services .............................. 78, 229, 330
- Disconnect Network Drives window .................................. 237, 245
- Display Settings window ..................................................... 23
- displaying the correct server .............................................. 203
- distribute Modular Messaging services across servers ...... 329
- DNS server .......................................................................... 157, 208
- DNS setup .......................................................................... 27
- documentation .................................................................... 5
  * library .............................................................................. 12
  * media ............................................................................... 12
  * requirements ................................................................... 9
  * Web access ...................................................................... 9
- doing acceptance tests ....................................................... 117, 120, 123, 124, 127, 241
- domain administrator account ......................................... 105, 107, 108, 109, 233, 236, 244
- Domain Admins group ........................................................ 223
- domain name
  * MSS administration ........................................................ 29
  * domain-wide feature setup ............................................. 54
  * Domino message store screen ......................................... 157, 208
- DSE
  * changing to H.323 ........................................................... 183
  * changing to QSIG .............................................................. 181
Index

changing to SIP ........................................ 184
DSE boards
  initial switch (PBX administration) ........ 15
DVD contents ........................................... 8

E
E1-QSIG boards
  cabling .............................................. 307
  configuring ........................................ 279, 310
  jumper settings .................................... 297
  plug for unused connector ....................... 293
  supported boards .................................. 277, 293
  testing ............................................. 287, 313
Edit a Class-of-Service page .................. 110, 111
edit TTS sessions .................................... 62
enabling services on the correct server ...... 338, 339
error logs on MAS ...................................... 81
Ethernet interface ....................................
event viewer 55, 69, 76, 77, 140, 161, 228, 239, 243, 287
Exchange message store screen ................. 157, 208

F
F1 key (help) ........................................... 5
Fax
  Configuring Microsoft Windows Fax service ... 70
  Moving Microsoft Windows Fax service ........ 334
Fax - Voice Mail Domain window ................. 68, 335
Fax Sender Server .................................... 68, 127, 336
fax service mailbox .................................. 110, 113
fax testing .......................................... 127
Fax User ............................................... 69

G
gateway to corporate network .................. 27, 157, 208

H
H.323
  changing from DSE or QSIG ....................... 183
  changing to SIP .................................... 187
  handoff procedures ................................ 143
hardware installation
  adding a new server ................................ 344
  cabling ............................................. 307
  port board cables .................................. 307
  preinstallation requirements .................... 295
help using the system ................................ 5
host information for MAS machines ............ 103, 232
how to use this book ................................ 3

I
IAS permissions ........................................ 19
IE .......................................................... 47
information on the Web ................................ 9
initial administration for PBX or switch and LAN 15
initial MSS administration
  logging in .......................................... 22
  monitor setup ...................................... 23
  MSS local machine profile ....................... 32
  MSS trusted servers ................................ 33, 35
  network addressing ................................ 27
  reboot MSS .......................................... 39
  set time and date .................................. 31
installation
  administering the MAS ............................. 41
  backing up the system ............................. 139, 141, 245
  checklist ........................................... 254
  configuring port boards ......................... 52, 275
  creating a new tone file ......................... 315
  hardware installation ............................ 291
  initial MSS administration ....................... 21, 101
  license ............................................. 61
  site requirements .................................. 7
  turning over system to customer ............... 143
installs
  client software updates .......................... 142
  integrated mode test .............................. 121
Intel Dialogic Configuration Manager window 279, 280, 282, 283, 310, 316, 319, 322
Intel Dialogic Configuration Manager, see Dialogic Configuration Manager
intended audience ...................................... 2
Internet alarming ..................................... 133
Internet Information Services (IIS), see also IIS Admin service .................... 88
IP address administration ......................... 27, 51, 130, 132, 221
IP H.323 integration ................................ 60, 275, 291, 308
IP SIP integration ................................. 275, 291, 308

J
join a Windows domain ............................. 233
join corporate Windows domain .................. 109
join private Windows domain .................... 108

K
KVM switch
  showing the correct server .................... 22, 203, 357

L
LAN

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

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>administration</td>
<td>27</td>
</tr>
<tr>
<td>initial administration</td>
<td>15</td>
</tr>
<tr>
<td>language preference on MAS</td>
<td>55</td>
</tr>
<tr>
<td>Languages - Voice Mail Domain window</td>
<td>71</td>
</tr>
<tr>
<td>LDAP</td>
<td></td>
</tr>
<tr>
<td>credentials</td>
<td>69, 219</td>
</tr>
<tr>
<td>enabling</td>
<td>37</td>
</tr>
<tr>
<td>password</td>
<td>32, 33, 345</td>
</tr>
<tr>
<td>Learn Tones window</td>
<td>318, 321</td>
</tr>
<tr>
<td>learning tones</td>
<td>315, 316, 319</td>
</tr>
<tr>
<td>license</td>
<td></td>
</tr>
<tr>
<td>obtain or install</td>
<td>60, 61</td>
</tr>
<tr>
<td>request file or support</td>
<td>60, 61</td>
</tr>
<tr>
<td>License Import wizard</td>
<td>61</td>
</tr>
<tr>
<td>Licensing - Voice Mail Domain window</td>
<td>62</td>
</tr>
<tr>
<td>links to other files</td>
<td>4</td>
</tr>
<tr>
<td>Linux Date and Time page</td>
<td>31</td>
</tr>
<tr>
<td>local machine profile setup</td>
<td>32</td>
</tr>
<tr>
<td>LocalSystem account</td>
<td>158, 209</td>
</tr>
<tr>
<td>Log On to Windows window</td>
<td>48, 356</td>
</tr>
<tr>
<td>logging in to MSS</td>
<td>22</td>
</tr>
<tr>
<td>logon accounts</td>
<td>130, 131, 157, 208</td>
</tr>
<tr>
<td>Logon accounts and passwords screen</td>
<td>158, 209</td>
</tr>
<tr>
<td>logs, changing default location</td>
<td>98</td>
</tr>
<tr>
<td>overview</td>
<td>41</td>
</tr>
<tr>
<td>preparing the server for service</td>
<td>47, 220</td>
</tr>
<tr>
<td>registering in ART</td>
<td>130</td>
</tr>
<tr>
<td>scheduling backups</td>
<td>139</td>
</tr>
<tr>
<td>setting up remote access</td>
<td>50, 221</td>
</tr>
<tr>
<td>showing the correct server</td>
<td>203</td>
</tr>
<tr>
<td>testing port boards</td>
<td>287, 313</td>
</tr>
<tr>
<td>updating host information on MSS</td>
<td>103</td>
</tr>
<tr>
<td>verifying basic operation</td>
<td>80</td>
</tr>
<tr>
<td>MAS backup file</td>
<td>236</td>
</tr>
<tr>
<td>MAS Backup window</td>
<td>140, 161, 243</td>
</tr>
<tr>
<td>MAS Host Information Setup page</td>
<td>103, 106, 232</td>
</tr>
<tr>
<td>MAS port board installation</td>
<td>305</td>
</tr>
<tr>
<td>MAS service account screen</td>
<td>158, 209</td>
</tr>
<tr>
<td>MAS services and features</td>
<td>158, 209</td>
</tr>
<tr>
<td>MAS-specific parameters</td>
<td>64, 74</td>
</tr>
<tr>
<td>maximum number of supported ports</td>
<td>293</td>
</tr>
<tr>
<td>Message Networking</td>
<td></td>
</tr>
<tr>
<td>enabling permissions</td>
<td>37</td>
</tr>
<tr>
<td>Message Servers - Voice Mail Domain window</td>
<td>69</td>
</tr>
<tr>
<td>Message store screen</td>
<td>157, 207</td>
</tr>
<tr>
<td>Message Waiting Indicator - Voice Mail Domain window</td>
<td>333, 336</td>
</tr>
<tr>
<td>Message Waiting Indicator (MWI), see MWI</td>
<td></td>
</tr>
<tr>
<td>Messaging - Voice Mail Domain window</td>
<td>73, 191, 224</td>
</tr>
<tr>
<td>Messaging Application Server Credentials</td>
<td>69</td>
</tr>
<tr>
<td>Messaging Application Server Number screen</td>
<td>45, 218, 351</td>
</tr>
<tr>
<td>messaging services to install</td>
<td>158, 209</td>
</tr>
<tr>
<td>Microsoft Windows activation</td>
<td>355</td>
</tr>
<tr>
<td>Microsoft Windows Fax service</td>
<td>70, 334</td>
</tr>
<tr>
<td>Microsoft Windows updates</td>
<td>14, 49, 90, 220</td>
</tr>
<tr>
<td>MISCM directory</td>
<td>136, 218, 346, 352</td>
</tr>
<tr>
<td>MM Aria interface</td>
<td></td>
</tr>
<tr>
<td>acceptance tests</td>
<td>122, 123, 127</td>
</tr>
<tr>
<td>set up on server</td>
<td>111, 114</td>
</tr>
<tr>
<td>MM Audit Service</td>
<td>67</td>
</tr>
<tr>
<td>See Audit Service</td>
<td></td>
</tr>
<tr>
<td>MM AUDIX interface</td>
<td></td>
</tr>
<tr>
<td>acceptance tests</td>
<td>122, 123, 127</td>
</tr>
<tr>
<td>set up on server</td>
<td>111, 114</td>
</tr>
<tr>
<td>MM Fax User</td>
<td>69</td>
</tr>
<tr>
<td>MM Serenade interface</td>
<td></td>
</tr>
<tr>
<td>acceptance tests</td>
<td>122, 123, 127</td>
</tr>
<tr>
<td>set up on server</td>
<td>111, 114</td>
</tr>
<tr>
<td>MM service selection screen</td>
<td>158, 209</td>
</tr>
<tr>
<td>MM_Setup window</td>
<td>356</td>
</tr>
<tr>
<td>modern</td>
<td></td>
</tr>
<tr>
<td>configuring</td>
<td>74</td>
</tr>
<tr>
<td>disconnect for upgrades</td>
<td>159, 247</td>
</tr>
<tr>
<td>RAS IP addresses</td>
<td>50, 130</td>
</tr>
<tr>
<td>Modern Dialout alarming</td>
<td>58, 74, 133</td>
</tr>
<tr>
<td>Modular Messaging Installation wizard</td>
<td>326</td>
</tr>
<tr>
<td>Modular Messaging services</td>
<td></td>
</tr>
<tr>
<td>balance across servers</td>
<td>329</td>
</tr>
<tr>
<td>disable</td>
<td>78, 229, 330</td>
</tr>
<tr>
<td>enable</td>
<td>338, 339</td>
</tr>
</tbody>
</table>

### M

- **Maestro** ........................................................................................................ 130
- **Mailbox Manager** .......................................................................................... 36, 37, 142, 248
- **Mailbox Monitor Server** ................................................................................
  - configuring Call Me and MWI ........................................................................... 65, 332
  - moving service .................................................................................................. 332
  - testing .................................................................................................................. 121
- **Manage Classes-of-Service page** ...................................................................
  - .......................................................................................................................... 110, 111, 216
- **Manage Local Administration Accounts page** .............................................. 216
- **Manage Local Subscribers page** ................................................................. 128
- **Manage Networked Machines page** ................................................................... 32
- **Manage Trusted Servers page** ........................................................................ 33, 35, 36, 345
- **Managing Subscribers page** ........................................................................... 112, 113, 114, 128
- **Map Network Drive window** ............................................................................ 236, 244
- **MAS** ...................................................................................................................
  - add new MAS to the system ............................................................................... 83, 100, 247, 253
  - adding a new server .......................................................................................... 341
  - balance MM services across servers ................................................................ 329
  - configuring a new server ............................................................................... 329
  - installing software updates ........................................................................... 349
  - restoring data .................................................................................................... 366
  - trusted server setup ......................................................................................... 234
  - updating MAS host information ........................................................................ 334
  - upgrades ............................................................................................................. 345
- **MAS accounts and passwords screen** ............................................................ 157, 208
- **MAS administration** .........................................................................................
  - access permissions ............................................................................................ 223
  - back up data ........................................................................................................ 139, 161
  - busyout ports ..................................................................................................... 159

372  Avaya Modular Messaging for Avaya MSS Release 5.0 Installation and Upgrades
moving among servers ............................. 331
restart ........................................ 76, 77, 226, 299, 339
start ........................................... 76, 77, 226, 299
stop ............................................ 76, 169, 235, 330, 338
testing services .................................. 241
verify correct services are started on MAS 228, 239
Modular Messaging User Properties window 55, 125, 126
monitor display quality .............................. 23
setup ........................................... 23
showing the correct server .......................... 22, 203
Monitor window ................................. 55, 76, 77, 226, 299, 330
monitoring tools for acceptance tests ............. 118
moving Modular Messaging services among servers 331
moving to corporate Windows domain after upgrade 188
MSS adding a new server .............................. 345
administering classes of service ..................... 110, 111
alarm origination .................................. 133, 135
assigning IP addresses ................................ 27
back up data ...................................... 141, 162, 212, 245
host name setup ..................................... 27
initial administration ................................ 21, 101, 130
installing software updates .......................... 326, 328
join a Windows domain (upgrade) .................... 233
join corporate Windows domain ....................... 109
join private Windows domain ....................... 108
local machine profile ................................ 32
logins and access .................................. 131, 132, 216
network addressing ................................... 27
placing MSS in Windows domain ....................... 108
rebooting ........................................... 39
registering in ART .................................... 130
restoring data ....................................... 213
setting up alarming ................................... 133
setting up logins .................................... 131
setting up remote access ............................... 130
setting up special mailboxes .......................... 110, 112
setting up subscribers ................................ 111, 114
trusted servers ..................................... 33, 35, 36, 157, 208, 345
updating MAS host information ....................... 103, 232
upgrading .......................................... 210, 231
upgrading to S3500-family server ...................... 213
MSS trusted server passwords screen ............... 157, 208
MWI configuring ..................................... 66
maximum number of sessions .......................... 76
moving service ...................................... 332, 333
testing operation .................................... 121, 127
trusted server ...................................... 35
nonintegrated mode test .............................. 123
Notify me ........................................... 65
NTP Time Server ...................................... 31

O
OAM .................................................. 59
obtain a license ...................................... 60
offline access feature ................................ 73, 191, 224, 225
offline access server ................................ 176
OLA ................................................ 176
ongoing system security ................................ 14
online help ......................................... 5
on-site security ....................................... 13
Operation History (OPH) viewer ....................... 82, 118
outcalling test ....................................... 124, 289

P
passwords
LDAP networking ....................................... 32
logon accounts ....................................... 157, 208
MSS logins .......................................... 131, 216
security ............................................. 13
patches to Avaya software ............................ 10, 116, 175, 240, 323
PBX
configuration notes 11, 53, 57, 75, 76, 222, 277, 308, 315
configuring .......................................... 57
initial administration .................................. 15
integration .......................................... 76
selecting integration .................................. 158, 209
supported integrations ................................ 57
test equipment ....................................... 14
PBXpert utility for tones file .......................... 315, 319
PBXpert wizard ....................................... 316, 317
performing pre-upgrade tasks ........................ 150, 205
permissions
Subscriber Administration window .................... 224
devices access ....................................... 191, 223, 224
System Administration window ........................ 191, 198, 223, 226
ping test .......................................... 105, 107
planning forms
upgrades ............................................ 155, 202, 206
verifying data to enter ................................ 345
verifying services to enable on a server 338, 339, 346
port boards
configuring 52, 76, 222, 275, 277, 279, 280, 308, 310, 311, 312
connecting cables .................................... 307
CPE servers ......................................... 293
disable ports on MAS .................................. 159
drivers and software .................................. 306, 308
enabling .............................................. 279, 281, 283, 310
ers. .................................................. 287, 289

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
cabling .................................................. 307
configuring ........................................... 280, 311, 312
jumper settings ......................................... 298, 299
supported boards ...................................... 277, 293
testing .................................................... 287, 313
setting up alarming .................................... 133
setting up MSS logins .................................. 131
setting up remote access .............................. 50, 130, 221
setting up the monitor .................................. 23
Shut Down Windows window .......................... 354
SIP
changing from DSE or QSIG ......................... 184
changing from H.323 .................................. 187
site requirements ....................................... 7
SNMP
alarming setup .......................................... 81, 133, 135
software
required for Modular Messaging ..................... 9
requirements ............................................. 9
shipped with system .................................... 8
software updates
installing ............................................. 10, 116, 175, 240, 323
obtaining .............................................. 10, 148, 202, 324, 363
special mailboxes on MSS ............................. 110, 112
Speech Access, see UCC SA .......................... 246
static IP addresses ..................................... 51, 221
Stop Messaging Software page ....................... 162, 214
Subscriber Options package
installing .............................................. 142, 248
testing outcalling ...................................... 124
supplementary server
adding ................................................... 344
administration ......................................... 33, 36
installing CPE server .................................. 291
support center (remote) ............................... 5
switch integration
changing boards during upgrade .................... 181
Switch integration screen ............................ 158, 209
switch, see PBX
Sysprep window ........................................ 45, 218, 351
System Administration page ........................ 37
system security ......................................... 13

t
cabling .................................................. 307
configuring ............................................. 280, 311, 312
jumper settings ......................................... 298, 299
supported boards ...................................... 277, 293
testing .................................................... 287, 313
TCP/IP port access .................................... 38
TCP/IP settings ........................................ 27, 103, 130, 132, 215, 232
technical assistance .................................... 5
technical support account ............................. 17, 19, 130, 158, 209
RAS and IAS permissions ............................. 19
technical support accounts ......................... 17
technical support staff ................................ 2
Telephone User Interface, see also MM Aria interface, MM AUDIX interface, MM Serenade interface, TUs .... 66
telephones for acceptance testing ................... 14, 120
Telephony Configuration wizard ...................... 75
Telephony Interface configuration ..................... 76, 222
Test Alarm Origination page ......................... 135
test equipment ........................................... 14, 120
test subscriber
adding ................................................... 114
initial switch (PBX administration) .................. 15
removing ................................................ 128
testing alarm origination ............................... 81, 135
testing outcalling capability .......................... 124, 289
testing port boards ..................................... 287, 313
testing server function ................................ 241
testing the system ...................................... 117, 241
Text-to-Speech (TTS) feature
enabling .................................................. 71
specifying sessions per MAS ......................... 62
verifying values ........................................ 158, 209
time and date setup .................................... 31
time zone settings ...................................... 31
tone file
backup .................................................. 236, 244, 318, 322
creating .................................................. 315, 319
restoring ............................................... 237
selecting ............................................... 284
Tracing Server service ................................. 336
verifying operation ..................................... 82
track messaging service startup ..................... 55, 76, 228, 239
trademarks ............................................... 4
training .................................................... 6
trusted servers
adding on MSS .......................................... 33, 35, 36, 345
MAS settings ............................................ 157, 208
TTST and announcements screen ..................... 158, 209
TUs
setup on MSS ............................................ 111, 114
turning over system to customer ..................... 143

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.
<table>
<thead>
<tr>
<th>Page(s)</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>241</td>
<td>acceptance tests</td>
</tr>
<tr>
<td>247, 253</td>
<td>add new MAS to the system</td>
</tr>
<tr>
<td>156</td>
<td>administering ports on switch</td>
</tr>
<tr>
<td>242</td>
<td>backing up MAS</td>
</tr>
<tr>
<td>161, 212, 242</td>
<td>backing up MSS</td>
</tr>
<tr>
<td>181</td>
<td>changing DSE or analog to QSIG</td>
</tr>
<tr>
<td>183</td>
<td>changing DSE or QSIG to H.323</td>
</tr>
<tr>
<td>184</td>
<td>changing DSE or QSIG to SIP</td>
</tr>
<tr>
<td>187</td>
<td>changing H.323 to SIP</td>
</tr>
<tr>
<td>185</td>
<td>changing QSIG T1 to QSIG E1</td>
</tr>
<tr>
<td>181</td>
<td>changing switch integrations</td>
</tr>
<tr>
<td>160, 211</td>
<td>check MAS spool directory</td>
</tr>
<tr>
<td>265</td>
<td>checklist</td>
</tr>
<tr>
<td>248</td>
<td>client software updates</td>
</tr>
<tr>
<td>242, 247</td>
<td>completing the upgrade</td>
</tr>
<tr>
<td>156</td>
<td>configuration notes</td>
</tr>
<tr>
<td>275</td>
<td>configuring port boards</td>
</tr>
<tr>
<td>217</td>
<td>MAS and supplementary Tracing server</td>
</tr>
<tr>
<td>188</td>
<td>move to corporate Windows domain</td>
</tr>
<tr>
<td>3, 4, 201</td>
<td>overview</td>
</tr>
<tr>
<td>220</td>
<td>preparing the server for service</td>
</tr>
<tr>
<td>150, 155, 205, 206</td>
<td>pre-upgrade tasks</td>
</tr>
<tr>
<td>244</td>
<td>remove old MAS backup files</td>
</tr>
<tr>
<td>228</td>
<td>restarting messaging service</td>
</tr>
<tr>
<td>213, 234</td>
<td>restoring data</td>
</tr>
<tr>
<td>277, 280, 311</td>
<td>supported port boards</td>
</tr>
<tr>
<td>232</td>
<td>updating host information on MSS</td>
</tr>
<tr>
<td>222</td>
<td>updating VMSC settings</td>
</tr>
<tr>
<td>210, 231</td>
<td>upgrading the MSS</td>
</tr>
<tr>
<td>213</td>
<td>upgrading to S3500-family server</td>
</tr>
<tr>
<td>228, 239</td>
<td>verify correct MM services are started</td>
</tr>
<tr>
<td>156, 207</td>
<td>verifying DCT data</td>
</tr>
<tr>
<td>325</td>
<td>inserting into server</td>
</tr>
<tr>
<td>81, 143</td>
<td>alarming connection</td>
</tr>
<tr>
<td>74</td>
<td>configuring</td>
</tr>
<tr>
<td>217, 349</td>
<td>getting system to recognize</td>
</tr>
<tr>
<td>24, 44, 136, 325, 346</td>
<td>inserting into server</td>
</tr>
<tr>
<td>137, 158, 209, 348</td>
<td>safely remove hardware</td>
</tr>
<tr>
<td>17, 19</td>
<td>user accounts</td>
</tr>
<tr>
<td>4</td>
<td>using links in this book</td>
</tr>
</tbody>
</table>

**Call Me Server** ........................................... 65, 332
**Fax Sender Server** ..................................... 68, 336
**Languages** .............................................. 71
**Licensing** ................................................ 60, 62
**Message Waiting Indicator Server** ...................... 66
**Messaging Application Servers** .......................... 74, 75, 76
**MWI Server** .............................................. 333
**Notify Me** ................................................ 65
**Offline Access** .......................................... 73
**PBXs** .................................................... 57, 76
**port boards** .............................................. 76, 222
**Security** .................................................. 223
**Serviceability** .......................................... 58, 74
**Telephone User Interface** ................................ 56
**Tracing Server** ........................................... 336

**voice mail domain** ........................................ 56, 64, 157, 207, 331, 336
**Voice Mail Domain screen** ................................ 157, 207
**Voice Mail System Configuration (VMSC)**, see VMSC
**Voice Mail System Configuration window** ............. 56, 57, 58, 60, 61, 62, 64, 69, 74, 75, 76, 222, 331, 336

**W**

**Web access to documentation** .............................. 9
**Web Client** ............................................... 18
**Web Client server**
  **updating** ............................................. 142, 248
**Web Subscriber Options**
  **installing on server** .................................... 158, 209
  **updating software** .................................... 142, 248
**Windows Components wizard** ................................ 88, 89
**Windows domain** ........................................... 233, 236, 244
**Windows Domain Setup page** .............................. 108, 109, 233
**Windows Internet Explorer** ................................. 47
**Windows product key** ..................................... 45, 218, 351, 354
**Windows Security window** ................................ 354
**Windows services** ........................................ 338
  **stopping** ............................................... 169, 235
**Windows Setup wizard** ................................... 45, 218, 351, 354
**WINS settings** ............................................ 157, 208
**World Wide Web Server, see Windows services** ........ 88

**V**

**verifying alarming setup** ................................ 81, 135
**verifying MAS call-handling ability** ..................... 80
**Verifying the private LAN** ................................ 28
**virtual memory size for MAS** .............................. 91
**virus-checking software** ................................ 14, 48, 220
**VMD ID, obtaining** ....................................... 60
**VMSC setup** ............................................... 53, 56, 64, 74, 222
  **Audio Encoding** ........................................ 56, 224