

Avaya Modular Messaging Release 3

System planning forms and installation or upgrade checklists for an Avaya MSS configuration

See the Avaya Support Web site for
the current issue of this document:
<http://www.avaya.com/support>

March 2006

Customer name:

Contact information:

Sold to:

You can use this editable file to enter planning information required for a new system installation or upgrade of an Avaya Messaging Application Server (MAS) in a Message Storage Server (MSS) configuration. This information is reproduced from *Avaya Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Release 3 Installation and Upgrades*, Issue 0.13, February 2006. These planning forms and checklists are not valid for any other issue of the Modular Messaging installation or upgrade documentation.

CAUTION: Use each set of planning forms only with the same issue of document that they support. Fields are added or changed between document releases. Do not remove any row (item numbers) from any of the planning form tables. If you do, the item numbers will not match the installation document, and you might enter bad data.

Information in this editable file includes:

- Appendix A: System planning forms
- Appendix B: Installation and upgrade checklists

Disclaimer: Avaya 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.

Appendix A: System planning forms

The installation of a new Avaya Modular Messaging system requires careful network planning to succeed. Server and domain information, account names, and passwords must be administered correctly on each server in the system. The customer *must* provide some information in advance, or the installation cannot proceed.

CAUTION: Use each set of planning forms *only* with the same issue of the document that they support. Fields are added or changed between software releases. The planning forms that support this issue of the *Installation and Upgrades* guide are different from planning forms that supported earlier releases.

You must license new systems using Remote Access Feature Activation (RFA). Authorized personnel must be trained in RFA and registered for Avaya Modular Messaging before they can request a license. For complete licensing steps and contact information for RFA assistance, see *Getting Started with RFA for Modular Messaging* on the <http://rfa.avaya.com> Web site.

Reviewing the planning forms and DCT data file

Check with your regional representative about the procedures you must use to submit and review the planning forms and the Data Collection Tool (DCT) data file. Avaya strongly recommends that an expert reviews this information before any installation or upgrade.

- In North America, the Solution Support Organization (SSO) Tier III group must review the planning information for accuracy and thoroughness. Send the completed set of planning forms and the DCT data file by e-mail to mmtac@avaya.com. Title the e-mail *MM Planning Forms for Tier III Review*. An SSO Tier III engineer reviews the information, notes any changes, and returns the forms and data file to the field contact.
- Avaya recommends that Business Partners also use the MMTAC organization to review their planning forms and DCT data files.

CAUTION: Installers update or complete the planning forms and DCT data file as part of a normal installation or upgrade. Ensure that you return any updated copies to the customer, the project planner, and the appropriate remote support organization.

Avaya recommends that Business Partners file their final, approved planning forms and DCT data files with the MMTAC organization. This action provides a backup of vital system information. However, Avaya advises Business Partners to specify that MMTAC representatives not dial in to systems that Business Partners maintain, unless previously authorized.

Note: You can use the DCT to help complete the information on the planning forms. The DCT program validates many entries and has online help. For more information, see *Using the Data Collection Tool (DCT)*.

Completing additional planning forms

You might need to complete additional planning forms for certain adjuncts. For the latest version of the planning forms, see the Avaya Support Web site at <http://www.avaya.com/support>:

- If the Modular Messaging system is to be networked to any legacy messaging systems through the Avaya Message Networking system, complete the corresponding Message Networking Planning Form. The network planning form is available on the documentation media for the Message Networking product.
- If a Unified Communication Center Speech Access (UCC SA) server is to be part of the system configuration, complete the planning forms for that server. See the appendix of the *Avaya Unified Communication Center Speech Access (UCC SA) Release 2.0.2 Site Preparation Guide* at <http://support.avaya.com/elmodocs2/ucc/R2.0/SPGuide.pdf>.

Terminology

The following terminology applies to the LAN administration process.

Alias. An alternate name for a computer host name or NetBIOS name.

Corporate LAN interface. Each Modular Messaging server has two network IP interfaces. One is connected to the LAN infrastructure constructed and maintained by the enterprise that purchased the system. This LAN is the corporate IP LAN and the Ethernet interface connected to it is the corporate IP interface. The corporate LAN gives the Modular Messaging server access to other computers and users.

Default IP gateway. The IP gateway to use if no other specified gateway is available. Each Modular Messaging server has at most one default gateway connected to the corporate IP interface. The private LAN does not use an IP gateway.

Domain name. A unique designator used to identify a group of related computers on the internet, such as *avaya.com*. Domain names are hierarchical, and the labels go from more specific on the left to more general on the right. A hierarchy can have any number of levels.

Domain Name Service (DNS). An Internet protocol service most often used to resolve symbolic names to IP addresses. The DNS service is constructed on hierarchical domains with different sets of servers serving each hierarchical layer.

DNS server. A computer that has the DNS service active. Such a computer can resolve symbolic names to an IP address for the DNS domain that the computer serves.

Full computer name. A complete name that identifies a specific Modular Messaging server on the corporate or private network. For more information, see *FQDN*.

Fully Qualified Domain Name (FQDN). A domain name that identifies an individual computer and the network on which the computer resides, such as *mymas1.loc.avaya.com*. The leftmost label is the primary name of the computer. This name is usually the host name, but not always. The FQDN is the same as the *Full computer name* for a Modular Messaging server.

Host name. The unique name of the computer. In Microsoft Windows terminology, this is often called the NetBIOS machine name. This name might or might not match one of the network interface names. The host name is often the short name of the public IP interface.

Initialization and Administration System (INADS). The Avaya program for remote service support. Support staff use INADS to monitor alarms and maintain installed systems.

IP address. A numeric value used to identify a computer connected to a network. If a computer has multiple network interfaces, it has multiple IP addresses, one for each connection to a different network. IP addresses are usually specified as four numbers separated by a period, such as *10.9.55.183*.

IP gateway. An IP address where IP packets are routed if the specified IP address is not on the network directly connected to the computer. An IP gateway is usually an interface on a router.

NetBIOS domain. A Microsoft Windows domain that is not fully qualified. This domain has no periods in the name, such as *privdom1*.

NetBIOS name. The Microsoft Windows term for a host name, also called a NetBIOS machine name.

Point-to-Point Protocol (PPP). An Internet standard protocol used for serial line connections, such as dial-up modems.

Private computer name. A name that identifies a server on the private network. The Modular Messaging software generates the private Windows domain name when the installation program configures MAS#1. The private full computer name contains the host name and the private Windows domain name, such as *mymas1.privdom1.local*.

Private LAN interface. The second network IP interface in each Modular Messaging server is connected to an Ethernet switch provided by Avaya as part of the product. The LAN is the private IP LAN and the Ethernet interface connected to it is the private IP interface. It is used only to send information between servers that make up the Modular Messaging system.

Public (corporate) full computer name. The corporate FQDN for a server. The name contains the host name and the complete public domain name, such as *mymas1.loc.avaya.com*.

Subnet mask. A numeric value used to tell which bits of an associated IP address are the network portion and which bits identify the specific host on the network. Each network interface has an IP address and an associated subnet (subnetwork) mask.

Voice Mail Domain (VMD). A group of one or more messaging application servers. Messaging (or voice) servers in a VMD share the VMD configuration properties and subscribers.

Windows domain. A grouping of network objects, such as users, groups, and computers. A Windows directory service called Active Directory stores all objects in a domain. Active Directory can reside on one or more domain controllers within a Windows domain.

Guidelines for completing the planning forms

Use the guidelines in this section to complete the planning forms for each Avaya Modular Messaging system that you must install or upgrade.

CAUTION: Keep a copy of the planning forms handy during system administration, and update them if information changes on the system during the installation or upgrade. File all records of passwords and account names securely.

Completing the Modular Messaging system planning form

Complete *Table 15: Modular Messaging system planning form* for each site. For more information about completing any fields, see the DCT online help system or the printed document, *Avaya Modular Messaging Data Collection Tool Online Help*.

CAUTION: For Release 3 upgrades, compare the new planning forms against the planning forms that are on file. Update any fields as needed. Verify all information against the actual system administration if possible. The upgrade erases all existing data.

Table 15: Modular Messaging system planning form

#	Item	Value	Notes
1	Name of company and organization		The system logon screen shows this information.
2	Message store to use	Avaya MSS	Required for this configuration.
3	Voice mail domain name—can be from 4 to 15 alphanumeric characters plus the special characters space, - , !£\$%^&*()~@		Use a simple unique term for the VMD that the software will create, such as <i>vmdom</i> .
4	Number of MASs, including optional supplementary Tracing server		Do not exceed 6 MASs for an MSS configuration.
5	Corporate network connection—choose one:	☐ Use static IP addresses (default) ☐ Obtain IP addresses using DHCP ☐ Do not connect to the corporate network	For details about corporate network setup, see <i>Table 16</i> .
6	Register the DNS suffix or the IP addresses for this connection in the DNS?	y/n ☐ Register this DNS suffix in the DNS? y/n ☐ Register the IP addresses for this connection in the DNS?	Specify for Dynamic Host Configuration Protocol (DHCP) connections only.
7	Static IP address range for Modular Messaging private network —choose one:	☐ 10.0.0.1 to 10.255.255.254 ☐ 172.16.0.1 to 172.31.255.254 ☐ 192.168.0.1 to 192.168.255.254	For details about private IP addresses based on address range, see <i>Table 19</i> .
8	Switch integration—choose one:	☐ Avaya CM (IP SIP) ☐ Avaya (IP H323) ☐ Avaya (QSIG) ☐ Cisco (QSIG) ☐ Nortel NT M-1 (QSIG) ☐ Siemens Hipath (QSIG) ☐ Other—specify: _____	
9	Folder for offline access to messages in a multiple-MAS system—specify the MAS and folder name:		Specify the offline message store used to synchronize messages. Use the format: \\mymas#\OfflineStore

Note: Make all domain names in the system unique to avoid confusion and to prevent possible problems in the network.

Completing the corporate network planning form

Complete *Table 16: Corporate network planning form* for each each Modular Messaging system. If you must install more than two MASs, also complete *Table 17: Corporate network planning form—additional MASs* for each additional server that you will install.

Note: For an example of a completed form, see *Example: Completed corporate network planning form*.

CAUTION: It is crucial to coordinate the IP addresses that will be used on the Modular Messaging servers with those on the corporate LAN. If you specify an Ethernet address for an Avaya server that conflicts with another Ethernet endpoint, the resulting traffic problems on the local area network can be extremely difficult to diagnose and solve. Work with the LAN administrator to identify and correct any potential addressing problems or conflicts.

To complete *Table 16* and, if required, *Table 17*:

1. Item **C1**: Choose unique NetBIOS machine (host) names for the MSS and all MASs, such as *mymss*, *mymas1*, and *mymas2*. You *must* keep track of what server you are administering. In this guide, *mymss* is the MSS, *mymas1* is MAS#1, and *mymas2* is a subsequent MAS. The optional supplementary Tracing server is *mymas6*.

CAUTION: The first MAS is promoted to a domain controller during installation, after which its name *cannot* change. Use its final name now.

Avaya recommends host (machine) names shorter than 10 characters long for ease in entering information online. The host name and domain name can each be 1 to 15 characters long. The complete computer name plus domain name must be 64 or fewer characters long, such as *mymas1.loc.avaya.com*. The computer host and domain names can be any unique term that complies with local conventions.

CAUTION: Use only numbers and lowercase characters for computer host names and domain names. Do not use any special characters except a hyphen (-). The first character *cannot* be a numeric character.

2. Items **C2** through **C10**: Enter the required corporate network information. The corporate IP or LAN administrator *must* supply these values. Corporate information includes:
 - The full corporate computer name for each server, also called the fully qualified domain name (FQDN)
 - All required IP addresses and domain names
 - Default gateway information, if used
 - Windows Internet Name Service (WINS) information, if used

Note: The corporate IP administrator must supply the IP address for any required DNS or WINS servers on the corporate LAN.

Guidelines for completing corporate information include:

- In Release 3, the MASs in a Modular Messaging system can use Dynamic Host Configuration Protocol (DHCP) to obtain their IP addresses automatically. If this site uses DHCP, do not supply IP addresses for Items **C4** and **C5** for the MASs or supplementary Tracing server.

CAUTION: You must assign a static IP address to the MSS, even if the system uses Dynamic Host Configuration Protocol (DHCP) to assign most IP addresses. The MSS also requires static IP addresses for any DNS servers in the search order.

- The corporate LAN administrator must supply the domain search order and any domain names in the required order. The LAN administrator must also provide any aliases for the Modular Messaging computers, if required for the corporate interface. The alias might be the host name of the computer, such as *mymas1*. An alias might also be some other NetBIOS name, such as *primname.loc.avaya.com*, depending on the corporate setup.

Note: All Modular Messaging servers must be in the same Windows domain and on the same LAN segment, whether provided by the customer or Avaya Inc. LAN personnel must configure IP addresses on the corporate DNS servers in keeping with local policy and practices. Customers must also register the corporate FQDNs for the MSS and each MAS on any relevant corporate DNS servers.

CAUTION: Do not use the same Data Collection Tool (DCT) data file for multiple systems in a networked environment. The name for the private Windows domain *must* be unique throughout the entire messaging network, or errors will occur. See Item **C11** in *Table 16: Corporate network planning form*. If the private domain name is duplicated anywhere in the network, you must reload all Modular Messaging software on all affected servers to correct the problem. Ensure that you use a unique private domain name on each Modular Messaging system.

Table 16: Corporate network planning form

#	Item	MSS	MAS #1	MAS #2
C1	Host name—machine or Windows NetBIOS name			
C2	Corporate domain name—use corporate-provided name			
C3	FQDN for corporate LAN interface—add primary server name, usually Item C1 , to the corporate domain name in C2 , such as <i>mymas1.loc.avaya.com</i>			
C4	IP address for corporate LAN interface—static connection			
C5	Subnet mask for corporate LAN interface—static connection			
C6	Aliases for corporate LAN interface, if required—system supplies host name by default			
C7	IP address for corporate default gateway			
C8	IP address for corporate DNS servers, if used			
C9	Search order of DNS domains			
C10	IP addresses for WINS servers, if WINS is required	—NOT USED—		
C11	Private Windows domain name ¹	—Use MAS #1 name—		—Use MAS #1 name—
C12	Full computer name for private LAN interface—add the host name in Item C1 to the private domain name in Item C11 , such as <i>mymas1.privdom1.local</i>			

¹ The Modular Messaging software creates a private Windows domain when it configures MAS#1, the domain controller. For a new system, record the private domain name after you configure MAS#1. The private domain name is the system-generated name just before the suffix *.local*, such as *privdom1.local*. For a system upgrade, record the privateWindows domain name that is already assigned. The existing private domain might not use a *.local* suffix.

Note: For a completed example of corporate network values for a two-MAS system, see *Example: Completed corporate network planning form*.

Table 17: Corporate network planning form—additional MASs

#	Item	MAS #3	MAS #4	MAS #5	MAS #6 ¹
C1	Host name—machine or Windows NetBIOS name				
C2	Corporate domain name—use corporate-provided name				
C3	FQDN for corporate LAN interface—add primary server name, usually Item C1 , to the corporate domain name in C2 , such as <i>mymas1.loc.avaya.com</i>				
C4	IP address for corporate LAN interface—static connection				
C5	Subnet mask for corporate LAN interface—static connection				
C6	Aliases for corporate LAN interface, if required—system supplies host name by default				
C7	IP address for corporate default gateway				
C8	IP address for corporate DNS servers, if used				
C9	Search order of DNS domains				
C10	IP addresses for WINS servers, if WINS is required				
C11	Private Windows domain name, new systems use <i>.local</i> suffix	—Use MAS #1 name—	—Use MAS #1 name—	—Use MAS #1 name—	—Use MAS #1 name—
C12	Full computer name for private LAN interface—add the host name in Item C1 to the private domain name in Item C11 , such as <i>mymas1.privdom1.local</i>				

¹ MAS#6, if present, can only be a supplementary Tracing server. This server handles certain services, but no calls.

CAUTION: This guide uses the sample entries in the following table for illustration purposes only. Do *not* use these values in your system!

Example: Completed corporate network planning form

#	Item	MSS	MAS #1	MAS #2
C1	Host name—machine or Windows NetBIOS name	mymss	mymas1	mymas2
C2	Corporate domain name—use corporate-provided name	loc.avaya.com	loc.avaya.com	loc.avaya.com
C3	FQDN for corporate LAN interface—add primary server name, usually Item C1 , to the corporate domain name in C2 , such as <i>mymas1.loc.avaya.com</i>	mymss.loc.avaya.com	mymas1.loc.avaya.com	mymas2.loc.avaya.com
C4	IP address for corporate LAN interface—static connection	10.9.83.214	10.9.83.72	10.9.83.73
C5	Subnet mask for corporate LAN interface—static connection	255.255.255.0	255.255.255.0	255.255.255.0
C6	Aliases for corporate LAN interface, if required—system supplies host name by default	mymss	mymas1	mymas2
C7	IP address for corporate default gateway	10.9.83.254	10.9.83.254	10.9.83.254
C8	IP address for corporate DNS servers, if used	10.9.1.39 10.9.1.2	10.9.1.39 10.9.1.2	10.9.1.39 10.9.1.2
C9	Search order of DNS domains	loc.avaya.com avaya.com	loc.avaya.com avaya.com	loc.avaya.com avaya.com
C10	IP addresses for WINS servers, if WINS is required	—NOT USED—	10.152.6.24 10.9.6.8	10.152.6.24 10.9.6.8
C11	Private Windows domain name	—Use MAS #1 name—	privdom1	—Use MAS #1 name—
C12	Full computer name for private LAN interface—add the host name in Item C1 to the private domain name in Item C11 , such as <i>mymas1.privdom1.local</i>	mymss.privdom1.local	mymas1.privdom1.local	mymas2.privdom1.local

Specifying private IP addresses

In Release 3, customers can specify one of three static IP address ranges to use for the private Windows network on the Modular Messaging system. Customers can therefore choose a range of IP addresses that does not conflict with other IP addresses used at their site. To select an address range, see Item 7 in *Table 15: Modular Messaging system planning form*.

In Release 3, the technician must enter the IP addresses manually on the Message Storage Server (MSS). However, the Avaya Modular Messaging Configuration Wizard configures each Messaging Application Server (MAS) automatically, using the data file from the Data Collection Tool. The private network settings and IP addresses on the MSS and MAS servers must match, or the Modular Messaging system will fail to work.

CAUTION: You must use the same private IP address range on the MSS that you will use on each MAS. Ensure that the settings in the data file for the Modular Messaging Data Collection Tool match the setting for Item 7 in *Table 15: Modular Messaging system planning form*.

Use *Table 18* and *Table 19* to find the IP addresses to use for each server, depending on the address range you selected. *Do not change these values unless absolutely necessary.*

Table 18: Private network settings for the Avaya MSS

Private network settings for MSS	Value
Private server name—do not change	mss1
IP address for 10.0.0.1 to 10.255.255.254 address range	10.255.1.1
IP address for 172.16.0.1 to 172.31.255.254 address range	172.31.1.1
IP address for 192.168.0.1 to 192.168.255.254 address range	192.168.1.1
Subnet mask—use for all IP address ranges	255.255.255.0

Table 19: Private IP addresses for each MAS by IP address range

Private network IP address range	MAS#1 IP address	MAS#2 IP address	MAS#3 IP address	MAS#4 IP address	MAS#5 IP address	MAS#6 ¹ IP address
10.0.0.1 to 10.255.255.254	10.255.1.250	10.255.1.249	10.255.1.248	10.255.1.247	10.255.1.246	10.255.1.245
172.16.0.1 to 172.31.255.254	172.31.1.250	172.31.1.249	172.31.1.248	172.31.1.247	172.31.1.246	172.31.1.245
192.168.0.1 to 192.168.255.254	192.168.1.250	192.168.1.249	192.168.1.248	192.168.1.247	192.168.1.246	192.168.1.245

¹ In an MSS configuration, any MAS greater than five must be a supplementary Tracing server. This server can handle special services, but no calls. Special services include Call Me Server, Message Waiting Indicator (MWI) Server, and Tracing Server. A supplementary Tracing server can also provide offline access to stored messages or host the Reporting Tool. Supplementary servers can use Avaya-provided hardware or customer-provided equipment (CPE).

Clients and optional applications

Make a checkmark next to the client packages and other optional applications that you want to use at this site. You must install all required client software after an installation or upgrade.

Table 20: Client and software applications for this site

✓	Client or software application	Notes
	Avaya Modular Messaging Subscriber Options, also known as the Modular Messaging (MM) Client	Recommended for each MAS
	Modular Messaging Web Client	Must be installed on its own server. You cannot install the Web Client on an MAS.
	Modular Messaging Web Subscriber Options—activate only once per voice mail domain (VMD)	☐ Install on its own server ☐ Install on the Web Client server ☐ Activate on an MAS, see <i>Table 24: MAS features list</i>
	IBM Lotus Notes Client	
	Microsoft Outlook Client	
	Standard IMAP client	☐ Enable LDAP? ¹ ☐ Use SSL? ☐ Use SMTP SSL? ²
	Standard POP3 client	☐ Enable LDAP? ☐ Use SSL? ☐ Use SMTP SSL?
	Unified Communication Center Speech Access	
	Networked Modular Messaging or Message Networking	
	Avaya Site or Multi-site Administration	
	Mailbox Manager	
	Provision	

¹ LDAP enables a client program to search for e-mail addresses based on subscriber names or telephone numbers.

² If a client uses Secure Sockets Layer (SSL) protocol, specify if SMTP SSL is also required.

Account and password tables

Complete the following tables with the customer to assign the passwords, account names, and login names for this site.

Note: Make account logon names and passwords site-specific for security reasons. Be sure to file records of passwords securely.

For all new installations, complete *Table 21: MSS local machine and trusted server passwords*. Record the customer-approved passwords for the MSS local server and all required trusted servers for the Modular Messaging system. Follow these guidelines when you create MSS passwords:

- Case is important for trusted server passwords. For best security, use a combination of uppercase and lowercase letters, numbers, and special characters or symbols.
- Passwords can be from 6 to 35 characters long. Avaya strongly recommends that passwords be at least 8 characters long.
- You can use special characters such as dash (-) for trusted server passwords. The following symbols were tested: ! # \$ % & ' () * + - . / : ; < > ? @ [] ^ _ { | } ~
Do *not* use the five symbols " , = \ ` Do *not* use any type of space character, deletion character, or other non-printable character. Avoid special characters in passwords for point-to-point or networked systems.

CAUTION: Do not create passwords composed of easily guessed words or numeric combinations, including sequential or repeated numbers. The DCT does not enforce compliance with the rules for special characters described in the previous bullet, so use care. Do not use the trusted server passwords for any other login.

Table 21: MSS local machine and trusted server passwords

#	MSS local machine or trusted server	Name of server on MSS	Name of service on MAS	Password
P1	MSS local machine—LDAP directory password for networking with other messaging servers	local <i>mssname</i>	—	
P2	Any MAS—all MASs and the supplementary Tracing server use the same password	trusted server <i>masname</i>	LDAP	
P3	Message Waiting Indicator (MWI) Server	trusted server VVSTS	MWI	
P4	IMAP trusted server	IMAP4 TUI	IMAP	

If any of the following applications are required, you can optionally set up the trusted server for them during installation. The customer must provide all required data in *Table 22*.

Table 22: Optional trusted servers

✓	MSS trusted server	Trusted server name ¹	Full computer name or IP address ²	Password
	Directory Enabled Management (DEM) Server	dem		
	Mailbox Manager	mbmserver		
	Provision	provision		
	Site Administration (ASA)			
	Speech Access (UCC SA)			

¹ Use lowercase for all server names. The names in the MSS and on the trusted server must exactly match.

² Provide the full computer name if the system uses DHCP. Use an IP address if the system uses static IP addresses.

Complete *Table 23: MAS logon accounts form*. Record all customer-provided account names and passwords required for this site.

Guidelines for MAS account names and passwords include:

- **Account names:** MAS account names must be between 7 and 32 characters long. In addition to alphanumeric characters, you can use the special characters underscore (_), period (.), and dash (-) in account names. You cannot use the symbols " / \ [] : ; | = , + * ? < > or space. The account name for each MAS must be unique. Case is not important for account names, although case does matter for passwords. **//True about case?//**

CAUTION: Avaya internal tools might not accept special characters. For the technical support account, use only numbers and uppercase and lowercase letters.

- **Passwords:** MAS passwords must be between 8 and 32 characters long. Avaya recommends that you make at least one of the first 7 characters a symbol or a punctuation mark. Do not use a pound sign (#) as the first character. Do *not* use a percent symbol (%) anywhere in the password. A password *cannot* contain the account name. **//What symbols are known to work?//**

CAUTION: Do not create passwords composed of easily guessed words or numeric combinations, including sequential or repeated numbers. You must use a combination of at least three of the following four character types: uppercase letters, lowercase letters, numbers, and special characters or symbols.

- Ensure that you are satisfied with Modular Messaging account names and passwords before you administer them. They are *not* easy to change later.
- Do *not* use the examples shown in this guide as the actual MAS account names. They are provided for example purposes only.

Note: For upgrades, you might have to change existing account names and passwords to comply with the Release 3 rules. You cannot proceed with an upgrade unless you enter compliant MAS account names and passwords into the DCT.

Using the Data Collection Tool (DCT)

You must enter MAS passwords and account names into the Avaya Modular Messaging Data Collection Tool (DCT) to do an installation or upgrade. The DCT follows the rules described in this section. The tool flags discouraged entries with a yellow (caution) highlight, and marks invalid entries in red. You must change any invalid entries before you can configure the system.

For more information about creating account names and passwords, see the help system for the Avaya Modular Messaging Data Collection Tool (DCT). This information is also available in the printed document *Avaya Modular Messaging Data Collection Tool Online Help*.

The Avaya Modular Messaging Data Collection Tool (DCT) is contained in a single executable file named **MMDCT.exe**. You can obtain a copy of the DCT from:

- the Avaya Support Web site at <http://www.avaya.com/support>
- Disk 1 of the Release 3 version of the *Avaya Modular Messaging Messaging Application Server Software* media. Navigate to the directory **Install\MISC**.

Table 23: MAS logon accounts form

#	Account	Logon name — customer specified	Password	Used for
A1	Domain administrator account for MAS#1—required ¹	<i>customer specified</i> such as dom-admin		Domain controller administration and system backups
A2	Local administrator account for MAS #2, if present	<i>customer specified</i> such as mas2-admin		Local administration for this MAS
A3	Local administrator account for MAS #3, if present	<i>customer specified</i> such as mas3-admin		Local administration for this MAS
A4	Local administrator account for MAS #4, if present	<i>customer specified</i> such as mas4-admin		Local administration for this MAS
A5	Local administrator account for MAS #5, if present	<i>customer specified</i> such as mas5-admin		Local administration for this MAS
A6	Local administrator account for MAS #6, if present	<i>customer specified</i> such as mas6-admin		Local administration for the optional supplementary Tracing server
A7	Technical support account for accessing any MAS	<i>customer specified</i> such as craft		Support group remote access account—use this account for ART
A8	Customer account for administering any MAS	<i>customer specified</i> such as custacct		Customer administration account

¹ The domain administrator account controls local administration on MAS#1. You also use this account to set up backups and to join the MSS to the Windows domain. You must update the password for the domain administrator account in all these places if you change the password.

CAUTION: The logon names in this table are invalid. If you enter these account names into the DCT, the program gives you a warning. Use customer-provided names.

MAS services and features

Working with the customer, fill out *Table 24: MAS features list* to specify the Modular Messaging services and optional features to install on each MAS. Guidelines include:

- If only one MAS is installed, put all required services on that computer. Check off the features to install in the MAS#1 column.
- If more than one MAS is installed:
 - If both Call Me and Message Waiting Indicator (MWI) service are to be installed at this site, they must be on the same MAS.
 - Install these services on the MAS with the fewest ports if possible.
 - Install these services on the MAS with the second fewest ports if the Tracing Server is to be installed. The Tracing Server places the greatest demand on an MAS.
 - If this system uses a supplementary Tracing server, you can place the Call Me and MWI services on the supplementary server.
 - Always put the Tracing Server on the MAS with the fewest ports, or on its own computer.
 - If this system uses a supplementary Tracing server, you can place the Call Me and MWI services on the supplementary server.
 - If the customer provides the server for this solution instead of Avaya Inc., see *Appendix H: Installing a customer-provided supplementary server* in the installation guide.

Note: For the recommended distribution of Modular Messaging services based on the number of MASs, see the *Avaya Modular Messaging Concepts and Planning Guide* (PDF 2 MB). The planning guide is available on the documentation media and from the Avaya Support Web site at <http://www.avaya.com/support>.

The Modular Messaging configuration program automatically installs the Caller Applications Editor on each MAS.

Up to five (5) Avaya MASs can handle calls. An additional *supplementary* Tracing server can provide special services such as Call Me, MWI, or Tracing Server service. Although the supplementary server is sometimes called an MAS, the server cannot handle calls. A supplementary Tracing server can use Avaya-provided or customer-provided hardware.

Note: Any customer-provided supplementary servers must meet the requirements defined in the *Avaya Modular Messaging Concepts and Planning Guide* (PDF 2 MB). Indicate on the planning form if a supplementary server uses customer-provided equipment (CPE).

CAUTION: The Modular Messaging Web Client, if used, always must be on its own server. This application *cannot* reside on any MAS or on the supplementary Tracing server.

Table 24: MAS features list

Modular Messaging service to install	Max. # of sessions: ¹	on MAS#1	on MAS#2	on MAS#3	on MAS#4	on MAS#5	on MAS#6 ²
Call Me Server Message Waiting Indicator (MWI) Server <i>Both Call Me and MWI use the Mailbox Monitor Server. All three services must be on the same server if any are installed. Activate these services only once per voice mail domain (VMD).</i>							
Fax Sender Server — <i>Activate only once per VMD. Currently unavailable for IP H.323 or IP SIP integrations.</i>							
Web Subscriber Options ³ —<i>If required on an MAS as this site, activate only once per VMD.</i>	N/A						
Tracing Server — <i>Activate only once per VMD.</i>	N/A						
Text-to-Speech —<i>If used, list all required languages.</i>		2	2	2	2	2	N/A
Messaging Application Server —<i>Activate on each MAS that is to handle calls.</i> Announcement languages —<i>At least one language is required for each MAS that is to handle calls.</i> Note: Install Subscriber Options on each MAS to facilitate remote support of subscribers.	N/A	Default language: List all languages to install:					

¹ Specify the maximum number of concurrent sessions for a feature based on expected usage. For guidelines, see the configuration notes and the *Avaya Modular Messaging Concepts and Planning Guide*.

² MAS#6 can only be a supplementary Tracing server that handles special services such as Tracing Server, Call Me, or MWI service. A supplementary server cannot handle calls. If this server is present, indicate if it is an Avaya-provided computer or customer-provided equipment (CPE).

³ You can run the Web Subscriber Options application on its own server, co-resident on an MAS, or co-resident on the Modular Messaging Web Client server, if used. The Modular Messaging installation program automatically installs Web Subscriber Options (WSO) on each MAS. To activate WSO on an MAS, indicate which MAS is to serve as the WSO web server. Activate WSO only once in the VMD.

Required switch and messaging information

Collect the required information from the relevant administrator before the installation. Always obtain the latest configuration notes for this particular switch (PBX) and integration from the Avaya Support Web site at <http://www.avaya.com/support>.

Table 25: Switch and messaging information

Item	Value	Notes
Type of switch or PBX: Integration method: Example: <i>Avaya Definity G3, T1 QSIG</i> .		Configuration note used for this integration: Number: Version: Date:
Record required switch integration information. Use the configuration note to determine required items, such as: IP address for IP SIP, IP H.323, and CLAN integrations. Switch trunk, signal, or hunt groups and routing pattern. IP address for SIP Enablement Services (SES) proxy server, required for IP SIP integrations		
If required for this integration, list the extension numbers for the ports on the MAS, and the switch ports to which they connect. Note: For greater reliability, distribute the port board extensions over several switch boards if possible. You might need to obtain the required information from the telephone system vendor.	<i>Use format: cabinet carrier slot port</i>	<i>Connects to extension number:</i>
Direct Inward Dialing (DID) numbers for: - MM hunt group for messaging services: - MSS alarm port number (RMB): - MAS modem dial-in number—one for each MAS - MAS#2, if present - MAS#3, if present, and so on Note: Provide complete dial-in number for each item.		
Number range for subscriber mailboxes in dial plan: Prefix, if required: _____ Number of digits in dial plan: _____	<i>Starting number:</i>	<i>Ending number:</i>
Are port groups required? Use configuration notes. If yes, supply group name, use, and number of ports. Example: <i>MWI outgoing only, 2 ports.</i>	<i>Port group 1 (Default):</i> Number of ports:	<i>Port group 2:</i> Number of ports:

Table 26: Mailbox and subscriber information

Item	Value
Telephone user interface: MM Aria (y/n)___ MM AUDIX (y/n)___ MM Serenade (y/n)___	
Postmaster mailbox: • Mailbox number—DID not required • Password—must be numeric • Class of service (cos) to use	
Fax mailbox number—must not be a real extension: • Password—must be numeric • Complete company fax machine number—DID • Class of service (cos) to use	
Test subscriber name for MM Aria: • Extension number to test telephone with DID • Password—must be numeric • Class of service (cos) to use	
Test subscriber name for MM AUDIX: • Extension number to test telephone with DID • Password—must be numeric • Class of service (cos) to use	
Test subscriber name for MM Serenade: • Extension number to test telephone with DID • Password—must be numeric • Class of service (cos) to use	
Additional mailboxes, if needed:	

Note: You can expand this table to include additional mailboxes that must be set up at time of installation. For example, you might include mailbox, password, community ID, class of service (cos), and other required information for:

- System broadcast mailbox
- System Enhanced-List Application (ELA) mailbox
- Other features or restrictions required for this site, such as Caller Applications

Support information

Fill out the appropriate sections, depending on how alarming is to be implemented at this site. You can use either the Avaya Initialization and Administration System (INADS) or a corporate Simple Network Management Protocol (SNMP) system.

Note: Because the MSS and MAS are separate servers, you can possibly implement one type of alarming for the MSS and another for the MAS servers. However, Avaya recommends that you use one type of alarming, either INADS or SNMP, across the entire Modular Messaging system.

General alarming information

Technical support information required for each installation includes:

- Alarming notification used at this site—INADS, SNMP, or none: _____
- Product ID number for MAS VMD: _____
- Product ID number for MSS: _____

Note: Product IDs must be ten numeric digits (0 through 9) long. The Avaya Automatic Registration Tool (ART) generates product IDs and RAS IP addresses for Avaya-supported servers when you register the system.

To enable remote support, record the RAS IP addresses for each MAS in the system, including the supplementary Tracing server, if present. Complete *Table 27* before an upgrade, or after you register a new system in ART.

Table 27: RAS IP addresses for each MAS

Modular Messaging Server	Starting IP address ¹	Ending IP address
MAS#1		
MAS#2		
MAS#3		
MAS#4		
MAS#5		
Supplementary Tracing server		

¹ For systems that Avaya maintains, use the ART-assigned IP address for the **Start** value, such as 10.27.00.29. Add 1 to create the **End** value, such as 10.27.00.30.

Complete *Table 28* at the time of the installation or upgrade, using the labels on the servers:

Table 28: MSS serial number and Windows product keys for MASs

Server	Windows Server Product key or MSS serial number
MSS Serial Number on rear port tray	
MAS#1 Windows product key	
MAS#2 Windows product key	
MAS#3 Windows product key	
MAS#4 Windows product key	
MAS#5 Windows product key	
Windows product key for supplementary Tracing server	

INADS alarming information

If INADS alarming is to be used at this site, supply the following information to allow the MAS modem to make outgoing calls:

- Communications (COM) port that each modem must use to make alarm notification calls. The port is COM3 for the recommended USB port on the MAS: _____
- Complete alarm destination telephone number: _____

Note: For a complete list of support numbers for all regions, see the Global Call Routing Guide at <http://toolsa.sd.avaya.com/directories/index.php?mode=crg>. For example, in North America, the INADs number is 1-800-535-3573.

- Modem setup (initialization) string required for the modem to make the alarm notification calls. For more information, see the documentation provided with the modem: _____

SNMP alarming information

If SNMP alarming is to be used at this site, supply the following information:

- Network Management Station IP address or fully qualified domain name. Specify the corporate network management system (NMS) that is to monitor the Modular Messaging system for alarm notifications (traps): _____
- Context (community) to which the NMS belongs. For more information, see the SNMP NMS documentation: _____
- Acknowledgement type: specify **Return Trap** to have the NMS actively acknowledge traps, or **Ping Surround** to have the MAS ping the NMS before and after sending a trap. If the pings succeed, the NMS is assumed to have received the trap: _____

Note: If SNMP alarming is used, the customer is responsible for providing and provisioning

the SNMP network management system. The customer must configure the SNMP system to receive and optionally acknowledge the traps that the Modular Messaging system generates.

MSS logins and PPP information

Use *Table 29* to record passwords for all required logins. If the login requires a point-to-point (PPP) remote access connection to the MSS modem, enter the required IP addresses.

Table 29: MSS logins, passwords, and PPP IP addresses

MSS login	Password ¹	Local IP address for PPP access through the MSS modem —customer provides	Remote IP address for PPP access through a remote modem—customer or remote support group provides
craftppp ²			
sapp, if customer requires this type of remote access			
dadmin, if required for Business Partner use		—	—
sa		—	—
vm		—	—

¹ For MSS administrative passwords, do not use the special characters quote ("), backslash (\), or backtick (`).

² For systems that Avaya maintains, MMTAC assigns the tscppp IP address and password.

CAUTION: The PPP IP addresses must not conflict with the network addressing scheme on the customer corporate network. For systems registered in ART, derive the PPP addresses from the ART-provided IP address. Subtract 1 from the initial IP address for each PPP IP address that is required, such as *10.27.00.28*.

Use *Table 30* only if you reload the operating system on the MSS. Usually you reload the MSS operating system only for upgrades or to correct system problems. For more information, see *Appendix F: Reloading the software on an MSS* in the installation guide.

Table 30: MSS software logins and passwords

MSS login	Password
root	
craft	
tsc	
sroot	
craftppp	

Note: ART automatically reassigns all the MSS software passwords in *Table 30* except *craftppp* when you register the system. The *craftppp* password must be the same as the one shown in *Table 29*.

Appendix B: Installation and upgrade checklists

These checklists can help guide you through the various installation and upgrade tasks.

- Before starting 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 them to ensure that you do not overlook any important tasks.

Unlike the planning forms, you can safely add or remove rows from the checklists. These checklists are planning aids that can help you customize an installation or upgrade for your particular site.

Checklists include:

- New Modular Messaging system installation
- Modular Messaging Release 3 upgrade

Note: If you are adding a new MAS to an existing Modular Messaging system, do the software upgrade *first* if an upgrade is required. After the upgrade is complete, install the new MAS using the new installation checklist.

New Modular Messaging installation

Use this checklist for a new Avaya Modular Messaging system installation. After you complete a task, make a checkmark in the column.

New Modular Messaging system installation checklist

✓	Description	Comments
	Complete the planning forms in Appendix A. Requires customer input from LAN, messaging, switch, and system administrators. Also complete any other relevant planning forms for Message Networking or UCC SA.	See the appropriate administrators. Planning forms are available from www.avaya.com/support .
	If Avaya is to maintain this system, pre-register the MSS in ART to get the product ID. Register each MAS in ART to obtain the server product ID and IP addresses for remote access.	You can obtain all required information for each MAS in advance.
	Obtain the DCT data file for this site, if available.	Local procedures vary.
	Assemble and review the required documentation.	Web access required.
	Download any required Avaya software updates.	Web access required.
	Review security issues.	
	Obtain the required anti-virus software for the MAS.	Customer obtains.
	Collect any software media that is needed for the installation, such as Microsoft Windows updates or anti-virus software.	Leave customer CDs and DVDs on-site.
	Gather the necessary tools and test equipment.	
	Arrange for LAN administration of the Modular Messaging system. Register MAS and MSS corporate computer names on the DNS. Note: Avaya Inc. is not responsible for the installation, administration, or test of communications between customer PCs and the LAN.	See LAN administrator. Time of administration and site requirements vary.
	Verify that the PBX or switch is administered.	See switch administrator.
	Review preinstallation site requirements, including: • Environmental requirements • Weight and space considerations • Customer-provided cabinet requirements • Installation area requirements • Power and grounding requirements • Demarcation points	
	Identify each S3500-family message server in the system.	Check and mark the label on each server.
	Unpack the Modular Messaging system hardware and peripheral components.	Open boxes as instructed to reuse packing materials.
	Attach mounting brackets and handles to the UPS and any EBM units as needed, and then cable the units together.	A UPS is always required. EBMs are optional.
	Attach the front bezel to each Avaya server.	
	Attach rails for rack-mount or rubber spacers for stackable configuration to each Avaya server.	Use appropriate method for this site.
	Connect the power cables for the system.	
	Connect the MAS port boards, if present, to the switch or PBX.	For more information, see the

		Dialogic documentation.
	Set up the MSS and MAS private LAN using an Ethernet crossover cable. Connect each server to the corporate LAN.	Optional configuration for a two-server system only.
	Connect a multiple-MAS system using an Ethernet switch: • Connect the MSS and first MAS only to the Ethernet switch for the private LAN. • Connect each server to the corporate LAN.	Do not connect subsequent servers to the private LAN until you are ready to configure them.
	Install the 2-port KVM switch, if used for a two-server system.	Do if required.
	Install the 8-port KVM switch, if present. Steps include: • Attach mounting brackets to KVM switch, if needed. • Connect KVM switch to the monitor, keyboard, and mouse. • Connect the KVM switch to each Avaya server.	Procedure varies, depending on type of KVM switch purchased.
	Set up the external modem for each MAS.	
	Connect the RMB, and its external modem if required, to the MSS and to the switch.	
	Turn on the Modular Messaging system and peripheral components.	
	Log on to the MSS.	
	Adjust the monitor settings if needed.	
	Set the date and time on the system.	
	Set up network addressing on the corporate and private LANs.	
	Set up the MSS local machine profile.	
	Administer all required trusted servers, including all MASs and the MWI trusted server, if this system uses MWI.	Use the planning forms.
	Administer the supplementary Tracing server, if present. Set up other optional trusted servers, if requested.	Do if required.
	Update the IMAP4 TUI password.	
	Enable required protocols for client application access.	
	Reboot the MSS.	
	Switch the monitor to show the correct MAS.	
	In the Modular Messaging configuration wizard, locate or create the data file for the Data Collection Tool (DCT).	Use the customer-provided data file if possible.
	Enter or verify the data in the DCT data file.	Do if required.
	Complete the Modular Messaging configuration wizard.	
	Install and administer anti-virus software.	Local procedures vary.
	Install the latest Avaya-approved updates for Microsoft Windows: system updates, security patches, and hot fixes.	Local procedures vary.
	Change the default names of the private and corporate LAN.	
	Enter the correct RAS IP addresses to allow remote access.	
	Record the private Windows domain name on planning forms.	Do on MAS#1.
	Configure and test the port boards if required, including: • <i>For analog boards</i>, create or use a valid tone file. • Configure each port board. • Test incoming and outgoing calls on each board.	Configuration notes required. Skip this step for IP-type or automatically configured integrations.
	Specify the preferred language for administration.	
	Verify that Modular Messaging service is started.	
	Use the Voice Mail System Configuration (VMSC) program to configure required domain-wide settings on MAS#1:	Do these tasks on MAS#1.

	• TUI and administration access settings • PBX parameters using the configuration notes • Serviceability settings for INADS or SNMP alarming	Configuration notes required for PBX settings.
	Use the VMSC to obtain the VMD ID needed for the license and submit request. Install the license file after delivery and set up TTS sessions for each MAS.	Local procedures vary.
	Configure specific features for this MAS, including: • Call Me, MWI, or Fax service • Languages or Text-to-Speech (TTS) • Offline access to messages—do only on last server	Set up the features and services that are required on each MAS or on the supplementary server.
	Configure specific parameters for this MAS, including: • INADS alarming, if used • Port boards and switch integration settings using the configuration notes. Service restart is required.	Do for each MAS. Configuration notes required.
	After VMSC configuration, restart messaging service. • Verify that all services not required on this MAS are disabled. Do not start all MM services until done. • Verify that all MM services required on this server are started and set to automatic.	Use the planning forms to ensure that only the correct services are enabled on each MAS.
	Restart service on all MASs in the VMD as a final step.	Do after last MAS.
	Verify the ability of each MAS to handle calls.	Not applicable for supplementary server.
	Verify the alarming setup on each MAS.	
	Verify Tracing Service operation, if installed on any server.	
	Install the Subscriber Options package on each MAS.	Server reboot when done.
	Switch the monitor to show the MSS.	
	Update the MAS host information.	Information varies for static IP addressing or DHCP.
	Place the MSS in the Microsoft Windows domain.	
	Set up a class of service for special mailboxes.	Postmaster is required.
	Set up a class of service for all required test subscribers.	MM Aria is the default.
	Administer the special mailboxes for the Postmaster and for fax, if fax service is installed.	
	Administer a test subscriber for all supported TUIs.	MM Aria is the default.
	Install any Avaya software updates, if needed.	Do if required.
	Set up monitoring tools to track calls, such as the operational history viewer, and port monitor for multiple-MAS systems.	Useful for troubleshooting.
	Do messaging acceptance tests, including: • Create and receive test messages in both integrated and nonintegrated mode. • Test all required TUIs. • Create and print faxes, if fax service is installed. • Test system outcalling using Subscriber Options.	Tests vary per MAS and local system setup.
	Remove any test subscribers.	

	Register the MSS in ART: • Activate the RMB external modem, if present. • With the modem active, register the MSS to program the product ID and remote access automatically. • Update MAS RAS information, if needed.	Required for all systems that Avaya supports.
	Set up logins and remote access on the MSS: • Administer required logins on the MSS to grant access to authorized parties. • Complete PPP server configuration.	Do as required.
	Specify INADS or SNMP alarm origination on the MSS, and test alarm origination.	Procedure varies for INADS or SNMP alarming.
	Do an attended backup on each MAS.	Do this on each MAS.
	Do an attended backup on the MSS. Discuss unattended backup methods with the customer.	Leave DVD backup in place.
	Install additional software or client applications if required.	Do if required.
	Copy the most current DCT data file to each MAS. Send a copy to the appropriate remote support organization.	Erase the data file from your USB drive when done.
	Ensure that the information on the planning forms is correct. Return the forms to the customer to file in a safe place.	Make a copy for the remote support organization.
	Hand off system to the customer for further administration.	

Modular Messaging Release 3 upgrade

Use this checklist when you upgrade an existing Modular Messaging Release 1.1 or Release 2 system to Modular Messaging Release 3 software. After you complete a task, make a checkmark in the column.

Note: If you must add a new MAS to an existing Modular Messaging system, do the software upgrade *first*. After the upgrade is complete, install the new MAS using the new installation checklist.

Modular Messaging Release 3 upgrade checklist

✓	Description	Comments
	Complete the planning forms in Appendix A. Requires customer input from LAN, messaging, switch, and system administrators. Also update any other relevant planning forms for Message Networking or UCC SA.	Use the latest planning forms to update those on file.
	Assemble and review the required documentation.	Web access required.
	Download any required Avaya software updates.	Web access required.
	Obtain the required anti-virus software for the MAS.	Customer obtains.
	Collect any software media that is needed for the upgrade, such as Microsoft Windows updates or anti-virus software.	Leave customer CDs and DVDs on-site.
	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.	Use the planning forms.
	Obtain and review the configuration notes for any changes.	Web access required.
	If you are to add an additional TUI to an MM Aria-only system, verify that MAS port maximums are within prescribed limits. If necessary, reallocate ports on the switch and in the MASs.	Do as required. Install any additional MASs only after the upgrade is complete.
	Switch the monitor to show the correct server.	
	Verify that all messaging servers and services are running.	
	Use the Data Collection Tool (DCT) to analyze each MAS.	Analyze all servers.
	Verify the DCT data file.	Save file on USB drive.
	Busyout the ports on the switch and MAS#1.	PBX procedures vary.
	Use the VMSC to add the Everyone group to Security.	Do on MAS#1.
	Do a fresh, attended backup on each MAS.	Do not use old backups.
	Do an attended backup on the MSS. You must stop service.	Make two copies.
	Unplug all system modems to prevent unneeded alarms.	
	Verify that the spool directory for MAS#1 is empty.	
	<i>Optional:</i> upgrade the MSS to an S3500-family server.	Do if required.
	Reload the operating system on an S3400-family MSS.	The hard disk is erased.
	Restore data on the MSS.	
	Verify basic system settings on the MSS.	
	Busyout and reroute the ports for this MAS if possible.	Use PBX procedures.

Verify that the spool directory for each MAS is empty.	
<i>Optional:</i> upgrade the server to S3500-family hardware. Move any MAS port boards to the new server.	Do if required.
Reload the operating system on an S3400-family server.	The hard disk is erased.
Activate the Microsoft Windows operating system.	Local procedures vary.
Copy the DCT data file to the hard disk before the next reboot.	
Run MM_Setup to prepare for automatic server configuration.	Turn on server afterwards.
Configure each MAS using the DCT data file.	
Install and administer anti-virus software.	Local procedures vary.
Install the latest Avaya-approved updates for Microsoft Windows: system updates, security patches, and hot fixes.	Local procedures vary.
Change the default names of the private and corporate LAN. Verify the search order of the two LANs.	Names vary depending on the hardware.
Enter the correct RAS IP addresses to allow remote access.	Do if required.
Wait for the FEDB resynchronization to complete.	Time varies.
Verify and update settings in the VMSC, including: • Update Security permissions for system administration. • Verify license settings and TTS sessions per MAS. • Verify port board and telephony interface settings. • Set up additional port groups, if required at this site.	Verify settings for switch integration and configured features as required.
Restart messaging service. • Verify that all services not required on this MAS are disabled. Do not start all MM services until done. • Verify that all MM services required on this server are started and set to automatic.	Use the planning forms to ensure that only the correct services are enabled on each MAS.
Restart service on all MASs in the VMD.	Do after last MAS.
Verify the ability of the MAS to handle calls.	
Upgrade each additional MAS. Use the most recent DCT data file to upgrade each subsequent server.	Repeat the MAS upgrade section as needed.
Update the MAS host information for each MAS.	
Place the MSS in the Windows domain.	Do this once per upgrade.
Verify the size and cos settings of the Postmaster mailbox.	Do this once per upgrade.
Set up classes of service and test subscribers for any additional TUIs that are required.	Do if required.
Stop all Modular Messaging services.	
Restore data on each MAS from most current backup.	
Restore Caller Applications for each MAS. //or MAS#1?//	Do if Caller Applications are used on the system.
Install any Avaya software updates, if needed.	Do if required.
Restart messaging service. Verify correct services are started.	
Repeat data restoration for each MAS.	
<i>Optional:</i> Set up monitoring tools to track test calls, such as the port monitor and operation history viewer.	Useful for multiple-MAS systems.
Do messaging acceptance tests, including: • Create and receive test messages in both integrated and nonintegrated mode. • Test all supported TUIs as required. • Create and print faxes, if fax service is installed. • Test system outcalling using Subscriber Options.	Tests vary per MAS and system setup.

	Do an attended backup on each MAS.	
	Remove old MAS backup files from the MSS.	Do this for each MAS.
	Do an attended backup on the MSS.	
	Add any new S3500-family servers to this system if required.	Use the new system installation checklist.
	Connect any unplugged modems to restore normal alarming.	
	Copy the most current DCT data file to each MAS. Send a copy to the appropriate remote support organization.	Erase the data file from the USB drive when done.
	Ensure that the information on the planning forms is correct. Return the forms to the customer to file in a safe place.	Make a copy for the remote support organization.
	Install any additional software required on this MAS, such as Mailbox Manager.	
	Update any installed MM client software on each computer where the software resides, such as the Subscriber Options package on each MAS.	Do as required. Local procedures vary.
	Install new client software, if required at this site.	Do if required.