Implementing Survivable Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Release 5.2

April 2011

Notice

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

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

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

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site:

http://www.avaya.com/support

License

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s)

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

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

Database License (DL). Customer may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicate with no more than a single instance of the same database.

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), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the 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 upon 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). Be aware that there might be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

- Your Avaya-provided telecommunications systems and their interfaces

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

TCP/IP Facilities

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

Standards Compliance

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

Federal Communications Commission Statement

Part 15:

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

Canadian Department of Communications (DOC) Interference Information

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

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

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

European Union Declarations of Conformity

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

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

http://www.avaya.com/support

Trademarks

Avaya is a registered trademark of Avaya Inc.

Aria, AUDIX, DEFINITY, INTUITY, and Serenade are registered trademark of Avaya Inc.

Mailbox Manager and COMPAS 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 142579.

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 1-800-876-2835 in the United States. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Contents

About this book

This book, Implementing Survivable Modular Messaging for the Avaya Message Store Server (MSS) configuration, Release 5.2, contains instructions for the following:

- Setting up and configuring the Avaya Survivable Modular Messaging system in an Avaya Message Store Server (MSS) configuration.
- Switching service to the Avaya Survivable Modular Messaging system when the primary Modular Messaging system becomes unavailable.
- Restoring service to the primary Modular Messaging system from the Survivable Modular Messaging system.
- Maintaining the readiness of the Survivable Modular Messaging system.

Note:

This book describes the Avaya Survivable Modular Messaging system only in an Avaya Message Store Server (MSS) configuration.

Intended audience

This book is intended primarily for experienced technical support staff who are responsible for setting up and configuring the Survivable Modular Messaging system. Additionally, the book is intended for customer support staff responsible for maintaining the Survivable Modular Messaging system and ensuring its readiness to take over messaging service.

The book frequently describes features and procedures that are also documented in other sections of the Release 5.2 documentation library. For more detail about the features and procedures, see the Modular Messaging, Release 5.2, documentation media.

How to use this book

This book is divided into five chapters:

- Chapter 1: System description on page 1.

  Contains a description of the Survivable Modular Messaging system and its requirements.

- Chapter 3: Installation and cutover checklists on page 25.

  Contains procedural checklists of the steps required to setup the Survivable Modular Messaging system, cutover service to the Survivable Modular Messaging system, and return service to the primary Modular Messaging system.

- Chapter 4: System maintenance checklist and requirements on page 55.

  Contains general maintenance guidelines and a checklist of the steps required to routinely restore data to the Survivable Modular Messaging system to keep it current with the primary system.

- Chapter 6: Checklist procedures on page 69.

  Contains detailed steps of the more complex procedures included in the checklists.

- Chapter 5: Survivable Modular Messaging planning form on page 65.

  Contains a planning form that must be completed with information required for the setup and maintenance of the Survivable Modular Messaging system. Most information most be completed before the setup can begin, though several fields are completed during the setup procedure.

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. Acronis is a trademark of Acronis, Inc. All other trademarks are the properties of their respective owners.

How to comment on this book

Avaya is interested in your suggestions for improving this information. Use one of the following methods to communicate with us:

Method	Contact
E-mail	infodev@avaya.com
Voice mail or fax	303-538-9625

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

Avaya Modular Messaging for Avaya MSS, Release 5.2, Survivable Modular Messaging Guide , November 2009.

Chapter 1: System description

Survivable Modular Messaging provides a disaster recovery solution for Modular Messaging Release 5.2 systems that use the S3500, S8730, S8800 1U, or HP DL360 G7 servers. With the backup and restore capabilities of Modular Messaging, users can create a duplicate of a primary Modular Messaging system. The duplicate includes messages, greetings, passwords, enterprise lists, Message Waiting Indicator (MWI) status and other data that is as recent as the latest backup and restore to the survivable system.

Survivable Modular Messaging is designed to work in conjunction with Avaya Aura^{TM} Communication Manager running on an Avaya Enterprise Survivable Server (ESS) or Avaya Local Survivable Processor (LSP).

Survivable Modular Messaging Release 5.2 now supports the MultiSite feature which allows you to use a single Modular Messaging system to serve subscribers at multiple locations. With MultiSite, MASs in a single Voice Mail Domain (VMD) communicate with multiple PBXs possibly with different dial plans, in different locations. MultiSite enables you to use a single Modular Messaging system consisting of many MASs to service a global organization. With MultiSite you can group distributed Modular Messaging sites under a single Voice Mail Domain (VMD).

In a MultiSite-enabled environment, the MASs are co-located with the Avaya MSS server in a data center, but the subscribers can be anywhere. The MASs communicate through the WAN with distributed SIP gateways that are installed near the PBXs at the various sites to service the subscribers. All MASs in the voice mail domain can handle requests from subscribers associated with any site and from any configured switch.

Survivable Modular Messaging Release 5.2 supports SIP integration. This allows Avaya Communication Manager with an Avaya Aura^{TM} SIP Enablement Services (SES) server or Avaya Aura^{TM} Session Manager 5.2 to communicate with Avaya Modular Message using SIP. Similarly, AudioCodes gateways can be used to connect to other PBXs.

Note:

For more information on the MultiSite feature and the concepts underlying MultiSite, such as sites and translation rules, see *Avaya Modular Messaging MultiSite Guide*.

See the following sections of this chapter for a description of the requirements for Survivable Modular Messaging:

- Hardware requirements on page 2
- Software requirements on page 2
- Configuration requirements on page 2
- Networking requirements on page 3
- Additional requirements on page 4

System requirements

This section gives the requirements that must be met to implement a Survivable Modular Messaging system.

Hardware requirements

The Survivable Modular Messaging system must meet the following hardware requirements:

- Both the primary Modular Messaging system and the Survivable Modular Messaging system must be running the S3500, S8730, S8800 1U, or HP DL360 G7 servers.
- The hardware configuration of the Survivable Modular Messaging system must be identical to that of the primary system. This includes an exact match in MSS, MASs, supplementary servers, Web Client servers, Web Subscriber Option servers, and Offline Access servers.
- The Survivable Modular Messaging system works in conjunction with an Avaya Enterprise Survivable Server (ESS) or Avaya Local Survivable Processor (LSP) that is running Avaya Communication Manager. Survivable Modular Messaging supports SIP, T1/E1 QSIG, and H.323 integration types.
- The Survivable Modular Messaging system works with other PBXs using Audiocodes SIP gateways.

Software requirements

The Survivable Modular Messaging system must meet the following software requirements:

- Both the primary Modular Messaging system and the Survivable Modular Messaging system must be running Avaya Modular Messaging Release 5.2 or greater software.
- The software configuration of the Survivable Modular Messaging system must be identical to that of the primary system. This includes all updates and patches to system software.

Configuration requirements

The Survivable Modular Messaging system must meet the following configuration requirements:

- The Survivable Modular Messaging system must reside on a different subnet from the primary Modular Messaging system.

- The primary system MSS must be configured for LAN backup to a local FTP server. An FTP server also must be available at the Survivable Modular Messaging location. Ideally, the primary system FTP server will be configured to automatically duplicate the latest MSS backup to the FTP server at the Survivable Modular Messaging location following each automatic nightly backup of the MSS.

  ⚠ **CAUTION:**

  Your FTP server must communicate correctly with the MSS. Validate the FTP server communication before attempting to install a Survivable Modular Messaging system. For more information, see Validating FTP server communication on page 70. If the validation test fails, contact your support organization before proceeding with the installation.

- For planning, use the following as a rough estimate of the size of the backup data that will be generated and sent across the WAN.

  Space used each night = 100 MB + 0.05 x (L+R) + 0.5 MB x L x F

  where:

  - L = the number of local subscribers on the system that night
  - R = the number of remote subscribers on the system that night
  - F = 1 if the system uses GSM, or 5 if the system uses G.711

  For example, a G.711 system with 2,000 local subscribers and 50,000 remote subscribers would have approximately 100 MB + 2,600 MB + 5,000 MB for a total of 7.7 GB of data.

- Client software must be configured to allow DNS to “look up” the address of the Modular Messaging system so that changes to the DNS server can easily route client access to the Survivable Modular Messaging system when necessary.
- Servers running the Web Client server and Web Subscriber Options must have the same host name on the primary and Survivable Modular Messaging systems.
- The same source file must be used to deploy caller applications on both the primary and Survivable Modular Messaging systems.
- If custom prompts change after the Survivable Modular Messaging system is created, they must be copied to the Survivable Modular Messaging system location and changed manually. Therefore, custom prompts are not recommended.

Networking requirements

The Survivable Modular Messaging system must meet the following networking requirements, if the system is networked:

- If the Survivable Modular Messaging system is part of a messaging network, then the Message Networking server is required.

- The Message Networking server must be configured to use DNS to “look up” the Modular Messaging system. Modular Messaging must be referenced by name only in the remote machine entry.

Additional requirements

The Survivable Modular Messaging system must meet the following requirements for setup to proceed:

- In the case of an existing system, the primary system must be fully installed and fully operational. If the primary system is newly installed, it must be fully installed, tested and ready for use.
- If Avaya PBXs are used, the following equipment must be available for setup.

Equipment	**Release**
Avaya Messaging Application Server S3500, S8730, S8800 1U, or HP DL360 G7	Modular Messaging Release 5.2
Avaya Messaging Storage Server S3500, S8730, S8800 1U, or HP DL360 G7	Modular Messaging Release 5.2
Avaya Web Client Server	Modular Messaging Release 5.2
Avaya Communication Manager running on an Avaya S8700 Media Server with G650 Media Gateway	Avaya Communication Manager Release 5.2
Avaya Communication Manager running on an Avaya S8500 Media Server with G650 Media Gateway	Avaya Communication Manager Release 5.2 (S8500-015-01.2.416.4)
Avaya SIP Enablement Services (SES) server or Avaya Session Manager	Release 5.2
Acronis Backup and recovery	Version 10
300GB or larger USB drive	II

  - A customer-provided copy of the software required to create a full bare-metal restore of the MASs and supplementary servers. One copy of the software is required for each server.
  - A copy of the Data Collection Tool (DCT) data file created at the time of the installation of the primary Modular Messaging System. The DCT data file has the extension mmdct, such as sitefile.mmdct. You will need the DCT data file to configure the MSS and each MAS. See Selecting or creating a DCT data file on page 75.

- A copy of the Survivable Modular Messaging Planning form that is completely filled out with the exception of the following fields. Enter the information in these fields during the installation procedure. Optionally, you can include the information for these fields in the **Notes** section of the DCT file.
    - Survivable Modular Messaging MSS and VMD product alarm IDs
    - Route pattern to Survivable Modular Messaging
    - Trunk Group to Survivable Modular Messaging
    - Trunk Group Trunk Access Code (TAC)
    - Survivable Modular Messaging MAS RAS IP addresses

Chapter 2: WebLM configuration for Survivable Modular Messaging system

Modular Messaging Release 5.2 uses Avaya Web License Manager (WebLM) as its standard licensing mechanism. WebLM is a Web-based licensing solution that facilitates license management.

Using WebLM, an administrator can track and manage licenses of multiple Avaya software products installed in an organization from a single location. The required license file resides on a WebLM Server and the license is tied to the MAC address of the WebLM Server.

A Survivable Modular Messaging system can either have one master WebLM Server or one master and two local WebLM Servers. You need to manage licenses between the master WebLM Server and the local WebLM Servers.

Note:

For more information on WebLM and WebLM configuration models, see *Installing and Configuring Avaya WebLM Server Guide.*

WebLM licensing modes for Modular Messaging

There are three license modes of WebLM:

- **License Normal mode**. In this mode, the system operates normally and any attempt to exceed the license parameters is denied.
- **License Error mode**. The system gets into License Error mode when it cannot contact the WebLM server, or there is a problem with the license. In this mode, you can perform any licensed operation, for a grace period of 30 days.
- **License Restricted mode**. The system enters License Restricted mode, if the problem is not fixed during the 30 day grace period in License Error mode. In this mode, you cannot enable any new subscribers for voice mail, nor make any changes to subscribers. Apart from these restrictions, the system operates normally. However, you can delete subscribers, if the licensed mailbox count is exceeds the specified limit.

Note:

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

Survivable Modular Messaging system modes

The Modular Messaging system can be in one of the following three modes.

- **Active**. In this mode, the Modular Messaging system is fully operational. This mode is appropriate for non-survivable systems and for the primary side of a survivable system. This is the default mode. In this mode, all license checks are performed against the WebLM server.
- **Standing by.** In this mode, the Modular Messaging system lies dormant, consuming no licenses, until aroused by an incoming phone call. This mode is appropriate for the non-active side of a Survivable Modular Messaging system.

  On setting this mode, the system releases all the acquired licenses and disables further license checks. After releasing the licenses, the system moves into the License Error mode. If there are no licenses to free (i.e. no licenses were previously acquired), the system continues in the existing mode. No new acquire licenses request or renew licenses request is performed.

  Note:
  Even though the system is not making any license request but once the system enters the License Error mode, the renewal thread stills performs the check for moving the system to License Restricted mode.

- **Active Alarm**. This mode is set by an incoming call on the survivable standby system. When the system is in survivable standby mode and the Common Caller Interface (CCI) detects an incoming call, the mode changes to survivable active alarmed by making a call on the license manager. In this mode, the Survivable Modular Messaging system handles calls and consume the licenses. This mode is similar to the **Active** mode but the only difference is a major alarm is raised to notify the administrator that now the Survivable Modular Messaging system is handling calls and its mode is changed to **Active Alarm**. Administrator should resolve the alarm.

  If the system is in License Restricted mode, the CCI does not allow subscribers to log on to mailboxes that are created but not initialized by working through the educator.

A Modular Messaging system enters the survivable **Standing by** mode only when the administrator sets it from the **Licensing** node in the VMSC. A Modular Messaging system leaves the survivable **Standing by** mode when the administrator changes the setting in the **Licensing** node in the VMSC to **Active**, or when it receives an incoming call.

A Survivable Modular Messaging system is optimally configured as a live system using the new survivable **Standing by** mode. Survivable **Standing by** mode improves the operation of a live Survivable Modular Messaging system, making a failover fully automatic.

For more information on configuring Survivable Modular Messaging system modes and resolving alarms, see *Messaging Application Server (MAS) Administration Guide*.

Survivable Modular Messaging system configurations

A Survivable Modular Messaging system can have three configurations:

- Standard configurations with periodic backup and restore
- Live Configurations
- Live Configurations with periodic backup and restore

Standard configurations

In Standard configurations, you regularly update the Survivable Modular Messaging system by restoring the backups created on the primary Modular Messaging system. Therefore, in a standard configuration the Survivable Modular Messaging system is always significantly out of date.

Following are the type of standard Survivable Modular Messaging configuration:

Figure 1: Standard configuration with one master WebLM Server

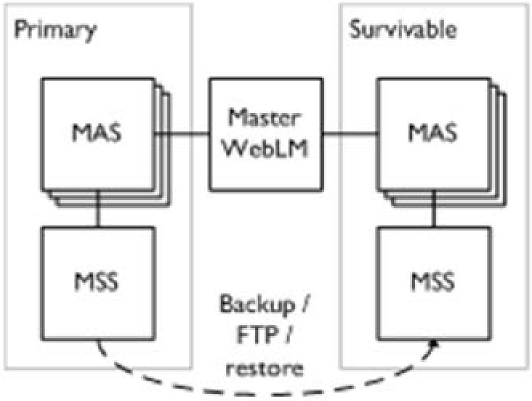
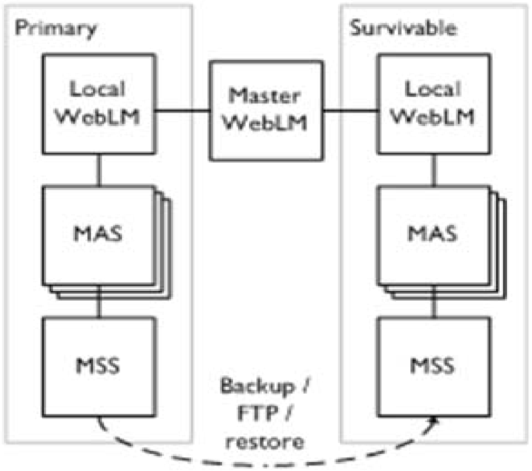


Figure 2: Standard configuration with one master WebLM Server and two local WebLM Servers



Live configurations

In a Live configuration, you can use a third-party product mirroring application to update the Survivable Modular Messaging system almost in real time whenever mailboxes on the primary system are changed. Licensing is more complex in this type of configuration than in standard configurations. However, the Survivable Modular Messaging system allows mailbox updates on the survivable system regardless of the licence mode of the survivable system.

Following are the type of Live Survivable Modular Messaging configuration using a third-party mirroring tool:

Figure 3: Live configuration with one master WebLM Server

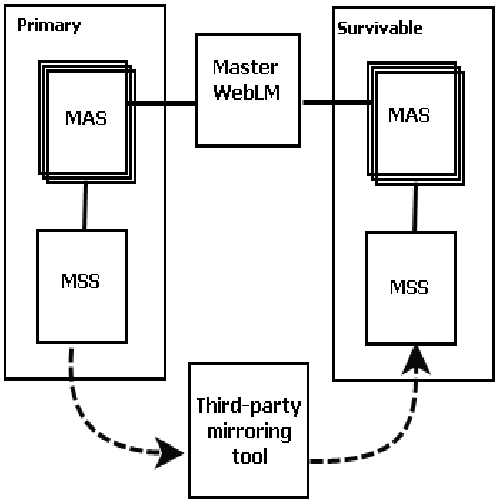
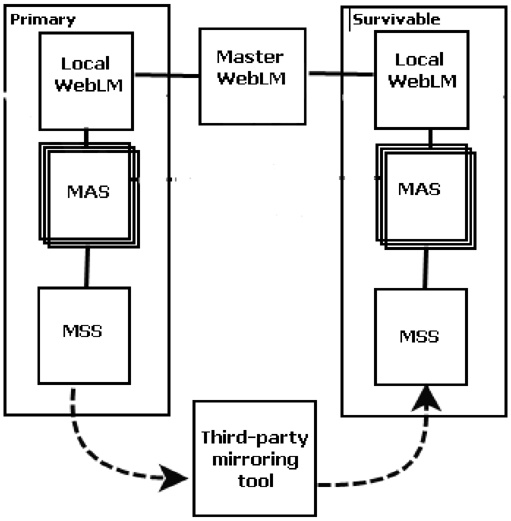


Figure 4: Live configuration with one master WebLM Server and two local WebLM Servers



Live configurations with periodic backup and restore

In this configuration type, most of the updates are in real-time, whenever mailboxes on the primary system are changed. However, some settings like PDLs get replicated only when you do the back up and restore.

Following are the type of Live Survivable Modular Messaging configuration using a third-party mirroring tool with periodic backup and restore:

Figure 5: Live configuration with periodic backup and restore with one master WebLM Server

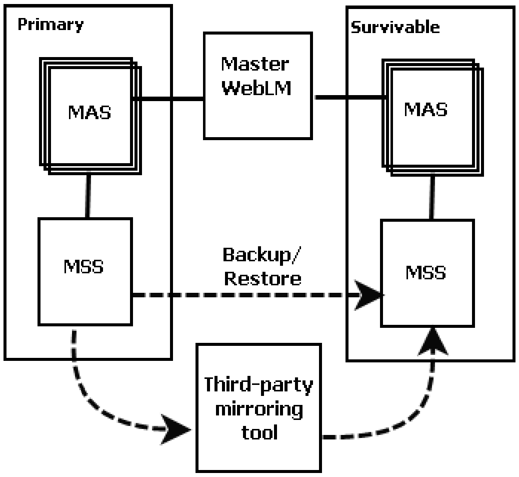
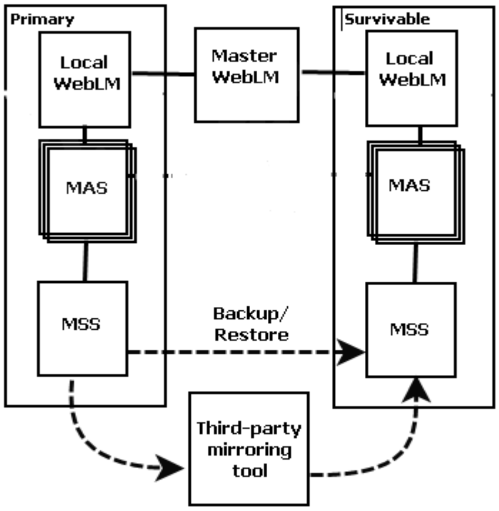


Figure 6: Live configuration with periodic backup and restore with one master WebLM Server and two local WebLM Servers



Survivable Modular Messaging system - License administration

License administration is very important on a Survivable Modular Messaging system. The Standing by mode influences the behaviour of License Error mode and License Restricted mode.

Note:
If you do not want to have a dedicated WebLM Server, Avaya recommends you to select any MAS on the Survivable Modular Messaging system as the master WebLM Server.

License administration for a Survivable Modular Messaging system with standard configuration

Table 1 gives an overview of licensing administration for the two WebLM Server topologies in a Survivable Modular Messaging system in a standard configuration.

Table 1: License administration for standard configuration

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
Normal operation		
Which WebLM Server controls the Modular Messaging mailbox licenses?	Master WebLM Server	Primary local WebLM Server
Where is the WebLM configuration of the primary Modular Messaging system done?	Master WebLM Server	Primary local WebLM Server

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
What should be the URL field of the Survivable Modular Messaging system WebLM configuration?	Master WebLM Server, with Modular Messaging in survivable standby mode.	Survivable local WebLM Server in survivable standby mode. This system has no licenses as all licenses are allocated to the primary local WebLM Server. You need to revoke the licenses from primary Local WebLM Server and assign them to survivable local WebLM Server at the time when the Survivable Modular Messaging system becomes Active from the Standing by mode. You can do this with in a period of 30 days, and during that period the Survivable Modular Messaging system runs in License Error Mode.
How to replicate the changes from primary Modular Messaging system to Survivable Modular Messaging system?	You must take a backup (using FTP) of the primary Modular Messaging system periodcally and restore it on the Survivable Modular Messaging system[1]. **Note:** After you restore the backup, move the Survivable Modular Messaging system to **Standing by** mode.	
Do you require periodic reconfiguration of licensing, to prevent the Survivable Modular Messaging system from entering the License Restricted mode?	Not required.	
Failover of primary Modular Messaging system		
What happens when the primary Modular Messaging system fails?	Licenses expire within 10 minutes and are reclaimed by the issuing WebLM Server.	

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
How are licenses reallocated to the Survivable Modular Messaging system when the primary Modular Messaging system fails?	Any incoming call triggers the system to change to the survivable active alarmed state. Then the Survivable Modular Messaging system attempts to acquire a valid license. If it is successful, it enters License Normal mode and if it fails, it enters License Error mode.	A WebLM administrator manually reallocates licenses from the primary WebLM Server to the Survivable local WebLM Server. Otherwise any incoming call triggers the system to change to the survivable active alarmed state. Then the Survivable Modular Messaging system attempts to acquire a valid license. If it is successful, it enters License Normal mode and if it fails, it enters License Error mode.
Is the Survivable Modular Messaging system available for taking calls when the primary Modular Messaging system fails?	Immediately, if the PBX has been appropriately configured, otherwise you need to manually reconfigure the PBX to redirect calls to the Survivable Modular Messaging system.	
Are the subscriber mailboxes on the Survivable Modular Messaging system in sync with the primary Modular Messaging system?	No, they are as the last restore done on the Survivable Modular Messaging system.	
Can mailbox settings be immediately configured on the Survivable Modular Messaging system?	Yes.	
Planned maintenance of the primary Modular Messaging system		
Are special steps required to stop the Survivable Modular Messaging system from acquiring licenses while the primary Modular Messaging system is down?	No, as long as no calls are directed to the survivable Modular Messaging system, it does not attempt to acquire any licenses.	No, because the licenses are controlled by the primary local WebLM Server and the licenses are not available to the Survivable Modular Messaging system.

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
Transfer operation back to the primary Modular Messaging system		
How to release the licenses from the Survivable Modular Messaging system?	Force the Survivable Modular Messaging system into survivable Standing by mode using VMSC. All licenses are released back to the master WebLM Server.	Use the master WebLM Server to pull back the Modular Messaging licenses from the survivable local WebLM Server. And, then change the Survivable Modular Messaging system to survivable Standing by mode.
How does the primary Modular Messaging system enters the License Normal mode?	The primary Modular Messaging system acquires the necessary licenses and then enters the License Normal mode.	

1. This statement assumes that the MSS allows to restore the backup even if the system is in a License Restricted mode.

License administration for a Survivable Modular Messaging system with live configuration

Table 2 gives an overview of licensing administration for the two WebLM Server topologies in a Survivable Modular Messaging system in a live configuration.

Table 2: License administration for a live configuration

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
Normal operation		
Which WebLM Server controls the Modular Messaging mailbox licenses?	Master WebLM Server	Primary local WebLM Server
Where is the WebLM configuration of the primary Modular Messaging system done?	Master WebLM Server	Primary local WebLM Server

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
What should be the URL field of the Survivable Modular Messaging system WebLM configuration?	Master WebLM Server, with Modular Messaging in survivable standby mode.	Survivable local WebLM Server in survivable standby mode. This system has no licenses as all licenses are allocated to the primary local WebLM Server. You need to revoke the licenses from primary Local WebLM Server and assign them to survivable local WebLM Server at the time when the Survivable Modular Messaging system becomes Active from the Standing by mode. You can do this with in a period of 30 days, and during that period the Survivable Modular Messaging system runs in License Error Mode.
How to replicate the changes from primary Modular Messaging system to Survivable Modular Messaging system?	Updates are almost in real-time, whenever mailboxes on the primary system are changed. **Note:** After you restore the backup, move the Survivable Modular Messaging system to **Standing by** mode	
Do you require periodic reconfiguration of licensing, to prevent the Survivable Modular Messaging system from entering the License Restricted mode?	Not required.	
Failover of primary Modular Messaging system		
What happens when the primary Modular Messaging system fails?	Licenses expire within 10 minutes and are reclaimed by the issuing WebLM Server.	

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
How are licenses reallocated to the Survivable Modular Messaging system when the primary Modular Messaging system fails?	Any incoming call triggers the system to change to the survivable active alarmed state. Then the Survivable Modular Messaging system attempts to acquire a valid license. If it is successful, it enters License Normal mode and if it fails, it enters License Error mode.	A WebLM administrator manually reallocates licenses from the primary WebLM Server to the Survivable local WebLM Server. Otherwise any incoming call triggers the system to change to the survivable active alarmed state. Then the Survivable Modular Messaging system attempts to acquire a valid license. If it is successful, it enters License Normal mode and if it fails, it enters License Error mode.
Is the Survivable Modular Messaging system available for taking calls when the primary Modular Messaging system fails?	Immediately, if the PBX has been appropriately configured, otherwise you need to manually reconfigure the PBX to redirect calls to the Survivable Modular Messaging system.	
Are the subscriber mailboxes on the Survivable Modular Messaging system in sync with the primary Modular Messaging system?	Yes, within a few minutes except for some user settings like the PDLs.	
Can mailbox settings be immediately configured on the Survivable Modular Messaging system?	Yes.	
Planned maintenance of the primary Modular Messaging system		
Are special steps required to stop the Survivable Modular Messaging system from acquiring licenses while the primary Modular Messaging system is down?	No, as long as no calls are directed to the survivable Modular Messaging system, it does not attempt to acquire any licenses.	No, because the licenses are controlled by the primary local WebLM Server and the licenses are not available to the Survivable Modular Messaging system.

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
Transfer operation back to the primary Modular Messaging system		
How to release the licenses from the Survivable Modular Messaging system?	Force the Survivable Modular Messaging system into survivable Standing by mode using VMSC. All licenses are released back to the master WebLM Server.	Use the master WebLM Server to pull back the Modular Messaging licenses from the survivable local WebLM Server. And, then change the Survivable Modular Messaging system to survivable Standing by mode.
How does the primary Modular Messaging system enters the License Normal mode?	The primary Modular Messaging system acquires the necessary licenses and then enters the License Normal mode.	

License administration for a Survivable Modular Messaging system with live configuration with periodic backup and restore

Table 3 gives an overview of licensing administration for the two WebLM Server topologies in a Survivable Modular Messaging system in a live configuration with periodic backup and restore.

Table 3: License administration for a live configuration with periodic backup and restore

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
Normal operation		
Which WebLM Server controls the Modular Messaging mailbox licenses?	Master WebLM Server	Primary local WebLM Server
Where is the WebLM configuration of the primary Modular Messaging system done?	Master WebLM Server	Primary local WebLM Server

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
What should be the URL field of the Survivable Modular Messaging system WebLM configuration?	Master WebLM Server, with Modular Messaging in survivable standby mode.	Survivable local WebLM Server in survivable standby mode. This system has no licenses as all licenses are allocated to the primary local WebLM Server. You need to revoke the licenses from primary Local WebLM Server and assign them to survivable local WebLM Server at the time when the Survivable Modular Messaging system becomes Active from the Standing by mode. You can do this with in a period of 30 days, and during that period the Survivable Modular Messaging system runs in License Error Mode.
How to replicate the changes from primary Modular Messaging system to Survivable Modular Messaging system?	Most of the updates are real-time, whenever mailboxes on the primary system are changed. However, there are some settings, like PDLs that get replicated when you do the back up and restore. **Note:** After you restore the backup, move the Survivable Modular Messaging system to **Standing by** mode	
Do you require periodic reconfiguration of licensing, to prevent the Survivable Modular Messaging system from entering the License Restricted mode?	Not required.	
Failover of primary Modular Messaging system		
What happens when the primary Modular Messaging system fails?	Licenses expire within 10 minutes and are reclaimed by the issuing WebLM Server.	

	Survivable standby mode with one master WebLM Server	Survivable standby mode with one master and two local WebLM Servers
How are licenses reallocated to the Survivable Modular Messaging system when the primary Modular Messaging system fails?	Any incoming call triggers the system to change to the survivable active alarmed state. Then the Survivable Modular Messaging system attempts to acquire a valid license. If it is successful, it enters License Normal mode and if it fails, it enters License Error mode.	A WebLM administrator manually reallocates licenses from the primary WebLM Server to the Survivable local WebLM Server. Otherwise any incoming call triggers the system to change to the survivable active alarmed state. Then the Survivable Modular Messaging system attempts to acquire a valid license. If it is successful, it enters License Normal mode and if it fails, it enters License Error mode.
Is the Survivable Modular Messaging system available for taking calls when the primary Modular Messaging system fails?	Immediately, if the PBX has been appropriately configured, otherwise you need to manually reconfigure the PBX to redirect calls to the Survivable Modular Messaging system.	
Are the subscriber mailboxes on the Survivable Modular Messaging system in sync with the primary Modular Messaging system?	Yes, within a few minutes except for some user settings like the PDLs.	
Can mailbox settings be immediately configured on the Survivable Modular Messaging system?	Yes.	
Planned maintenance of the primary Modular Messaging system		
Are special steps required to stop the Survivable Modular Messaging system from acquiring licenses while the primary Modular Messaging system is down?	No, as long as no calls are directed to the survivable Modular Messaging system, it does not attempt to acquire any licenses.	No, because the licenses are controlled by the primary local WebLM Server and the licenses are not available to the Survivable Modular Messaging system.

	Survivable standby mode with one master WebLM Server	**Survivable standby mode with one master and two local WebLM Servers**
Transfer operation back to the primary Modular Messaging system		
How to release the licenses from the Survivable Modular Messaging system?	Force the Survivable Modular Messaging system into survivable Standing by mode using VMSC. All licenses are released back to the master WebLM Server.	Use the master WebLM Server to pull back the Modular Messaging licenses from the survivable local WebLM Server. And, then change the Survivable Modular Messaging system to survivable Standing by mode.
How does the primary Modular Messaging system enters the License Normal mode?	The primary Modular Messaging system acquires the necessary licenses and then enters the License Normal mode.	

Upgrading Survivable Modular Messaging system to Modular Messaging Release 5.2

To upgrade a Survivable Modular Messaging system to Modular Messaging Release 5.2, perform the following steps:

1. Upgrade each Survivable Modular Messaging system to Modular Messaging Release 5.2 by following the standard non-survivable procedure.
    a. First, upgrade the Survivable Modular Messaging system. While doing the upgrades, if the primary Modular Messaging system fails, the Survivable Modular Messaging system is unavailable.
    b. Then upgrade the primary Modular Messaging system.

    Note:
    For more information on upgrade procedures to Modular Messaging Release 5.2, see *Avaya Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Release 5.2 Installation and Upgrades.*

2. Install the master WebLM Server.

    Note:
    For more information on WebLM Server installation, see *Installing and Configuring Avaya WebLM Server Guide.*

3. Install the local WebLM Servers.

    Note:
    Perform step 3 only if you have a one master WebLM Server and two local WebLM Servers Survivable Modular Messaging system configuration.

4. Get a new license with NIC ID of the master WebLM Server.
5. Perform one of the following steps:
    a. For one master WebLM Server and two local WebLM Servers Survivable Modular Messaging system configuration - install the new license and delegate the licenses to the WebLM Server on the primary Modular Messaging system.
    b. For one master WebLM Server Survivable Modular Messaging system configuration - install the new license and point the primary MAS to the master WebLM server and move the Survivable Modular Messaging system to **Standing by** mode

Chapter 3: Installation and cutover checklists

This chapter contains procedural checklists for each stage of the setup and use of the Avaya Survivable Modular Messaging system. Refer to Chapter 4: System maintenance checklist and requirements on page 55 for the procedures required to maintain the Survivable Modular Messaging system.

This chapter includes the following checklists:

- Capturing primary Modular Messaging system information on page 26
- Setting up the Survivable Modular Messaging system on page 29
- Switching service to the Survivable Modular Messaging system on page 39
- Returning service to the primary Modular Messaging system on page 44

Capturing primary Modular Messaging system information

To set up a Survivable Modular Messaging system you must first retrieve system information from the primary Modular Messaging system. Complete the steps in this checklist to retrieve the required information from the primary system MSS, MASs, and supplementary server.

All procedures described in this checklist are completed at the location of the primary Modular Messaging system.

Prerequisites

Before you can complete the procedures in this checklist, the following conditions must be met:

- The primary system must be fully installed, tested and ready for use.
- In case of a MultiSite system, all configurations required to enable the MultiSite feature such as configuring sites, site groups, PBX integration, and translation rules must be complete. For detailed procedures, see *Avaya Modular Messaging MultiSite Guide*.
- All hardware in the primary Modular Messaging system must be from the S3500, S8730, S8800 1U, or HP DL360 G7 server, running Modular Messaging 5.2 or later software.
- The primary MSS must be configured for LAN backup to a local FTP or SFTP server.
- The local FTP or SFTP server should be configured to replicate data to an FTP or SFTP server at the Survivable Modular Messaging location.
- The primary Modular Messaging system must be using DNS names for client access and networking, if applicable. Ensure that Fully Qualified Domain Name (FQDN) and IP address information on the customer's DNS server point to the IP addresses assigned to the servers in the primary Modular Messaging system. See the Survivable Modular Messaging planning form for DNS server information.
- For systems with SIP integration, a SIP trunk must be configured on the Avaya Communication Manager. All configurations required to connect the primary Avaya Modular Messaging system to the Avaya SIP Enablement Services (SES) server or Avaya Session Manager must be complete.

Additional requirements

To complete the procedures in this checklist, you must have the following:

- 300GB or larger USB II drive.

- A customer-provided copy of the software required to create a full bare-metal restore of the MASs and supplementary servers. One copy of the software is required for each server. For more information see Using Acronis Backup and recovery on page 72.
- A copy of the DCT data file created at the time of the installation of the primary Modular Messaging System. The DCT data file has the extension mmdct, such as sitefile.mmdct. You will need the DCT data file to configure the MSS and each MAS. See Selecting or creating a DCT data file on page 75.
- A copy of the Survivable Modular Messaging Planning form that is completely filled out with the exception of the following fields. Information will be entered in these fields during the installation procedure. Optionally, you can include the information for these fields in the **Notes** section of the DCT file.
    - Survivable Modular Messaging MSS and VMD product alarm IDs
    - Route pattern to Survivable Modular Messaging
    - Trunk Group to Survivable Modular Messaging
    - Trunk Group Trunk Access Code (TAC)

Checklist

Table 4: Capturing primary Modular Messaging system information

✔	**Steps**
	Validate FTP server communication. If the validation test fails, contact your support organization before proceeding with the installation. For instructions, see Validating FTP server communication on page 70.
	Create a folder share called SMM-Share$. For instructions for creating the folder, see Creating the SMM-Share$ folder on page 71.
	Create 2 copies of the bootable rescue media DVD. For instructions about how to create these DVDs using Acronis Backup and recovery software, see Creating bootable media on page 72.
	Connect the USB II drive to MAS 1.
	Create an image of MAS 1 on the USB II drive. For instructions about how to create the image using Acronis Backup and recovery software, see Creating backup image of MAS 1 on page 72.

Table 4: Capturing primary Modular Messaging system information

✔	Steps
	Create an image of each additional MAS and supplementary server in the system on the USB II drive.
	Detach the USB II drive and arrange with the customer for the drive to be transported to the Survivable Modular Messaging location. Alternately, you can arrange to carry the drive to the Survivable Modular Messaging location.
	Verify that the MSS is set up for LAN back up. To verify LAN back up, complete the following steps: 1. Log on to the MSS. 2. From the MSS Messaging Administration menu, select **Backup/Restore > Configure Remote Storage**. 3. In the **Backup Mode** field, verify that FTP or SFTP is selected. See *Administering remote storage for MSS backup* on the Modular Messaging, Release 5.2 documentation media for additional instructions about setting up MSS backup to the FTP or SFTP server.
	Conduct a full attended back up of the MSS. To conduct a backup, complete the following steps: 1. From the MSS Messaging Administration menu, select **Backup/Restore > Backup**. If you did not stop the messaging software before starting the backup, the system displays a warning message. Click **Continue Backup** to continue without stopping the messaging software, or click **Stop Voice System** to exit the Backup page and stop the messaging software. 2. Select **yes** from the drop-down list for all data types to ensure a full backup. 3. Click **Start Backup**. 4. Click **Continue** after verifying information the system displays about the backup. 5. Verify that the system displays a message that the full backup has been successfully completed. 6. Click **Return to Main**. For more information, see *Performing an attended backup to a remote storage location* on the Modular Messaging, Release 5.2, documentation media for detailed instructions.
	Arrange with the customer for a replication of the full MSS backup data from the local FTP/SFTP server to the one at the Survivable Modular Messaging location. Verify that the customer has provided the Survivable Modular Messaging location FTP/SFTP access information in the Survivable Modular Messaging planning form.

Setting up the Survivable Modular Messaging system

Complete the steps in this checklist to initially setup the Survivable Modular Messaging system.

All procedures described in this checklist are completed at the location of the Survivable Modular Messaging system.

Prerequisites

Before you can complete the procedures in this checklist, the following conditions must be met:

- You must have completed the steps described in Capturing primary Modular Messaging system information on page 26.
- The customer must have replicated the full backup of the primary MSS from the FTP/SFTP server at the primary Modular Messaging system location to the FTP/SFTP server at the Survivable Modular Messaging location.
- Installation of the Survivable Modular Messaging system hardware including all physical LAN connections must be complete. Hardware must exactly match the hardware configuration of the primary Modular Messaging system. For more information about installation procedures and requirements, see *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration, Release 5.2, Installation and Upgrades.*
- The Survivable Modular Messaging system must be installed in a different subnet than the primary Modular Messaging system.
- The Survivable Modular Messaging system must be configured to use a private Windows domain on the private network.
- Installation and configuration of additional servers for system functions that will not reside on an MAS or the supplementary server must be complete. For example, installation may include servers for the Web Client, Subscriber Options, or Web Subscriber Options if it does not reside on an MAS. These servers are not replicated as part of the instructions described in this manual. Follow normal installation procedures for these servers.

  Customer-provided servers in the Survivable Modular Messaging system must have the same host name as the corresponding server in the primary Modular Messaging system.

Additional requirements

To complete the procedures in this checklist, you must have the following:

- The USB II drive with images of the primary system MASs and supplementary servers. This USB II drive should have been shipped or hand carried from the primary location following completion of the steps described in Capturing primary Modular Messaging system information on page 26.

- A customer-provided copy of the software required to restore the images of the MASs and supplementary servers. One copy of the software is required for each server. For instructions, see Restoring the MAS image on page 73
- A copy of the Survivable Modular Messaging planning form that is completely filled out with the exception of the following fields. Information will be entered in these fields during the installation procedure. Alternatively, you can also enter the information for the following fields in the Notes section of the DCT file.
    - Survivable Modular Messaging MSS and VMD product alarm IDs
    - Route pattern to Survivable Modular Messaging
    - Trunk Group to Survivable Modular Messaging
    - Trunk Group Trunk Access Code (TAC)
    - Survivable Modular Messaging MAS RAS IP addresses
- A copy of the DCT data file created at the time of the installation of the primary Modular Messaging System. The DCT data file has the extension mmdct, such as sitefile.mmdct. You will need the DCT data file to configure the MSS and each MAS. See Selecting or creating a DCT data file on page 75

Checklist

Table 5: Setting up the Survivable Modular Messaging system

✔	Steps
	Register the Survivable Modular Messaging system using the ART tool. Record the product alarm IDs for the MSS and Voice Mail Domain (VMD) and the MAS RAS IP address for each MAS on the Survivable Modular Messaging planning form.
	Administer Avaya Communication Manager on the Enterprise Survivable Server (ESS) or Local Survivable Processor (LSP), or Avaya SIP Enablement Services (SES) server with a trunk group to be used exclusively by Survivable Modular Messaging. Do not route calls to this trunk group at this time. Record the number of the trunk group and the trunk access code (TAC) on the Survivable Modular Messaging planning form. For more information about creating the trunk group, see the configuration notes CN88015 for H.323, CN88003 for T1, CN88004 for E1, and CN88010 for SIP integration types. Download the latest versions from http://www.avaya.com/support. For more information about Avaya Enterprise Survivable Servers (ESS), see *Avaya Enterprise Survivable Servers User Guide*. For more information about Avaya SIP Enablement Services server see *Installing, Administering, Maintaining And Trouble Shooting Avaya Aura SIP Enablement Services*. Download the latest versions from http://www.avaya.com/support.
	Log on to the MSS.
	Change the MSS host name and IP address to match the host name and IP address of the primary MSS. To change the name and IP address, complete the following steps: 1. From the MSS Messaging Administration menu, select **Server Administration > TCP/IP Network Configuration > Configure Network Addressing**. 2. In the **Host Name** field, type the name of the primary MSS recorded on the Survivable Modular Messaging planning form. 3. In the IP Address field, type the MSS IP address recorded on the Survivable Modular Messaging planning form. 4. Click **Save**. 5. Click **Return to Main**. For more information, see Revising MSS IP addresses on page 78

Table 5: Setting up the Survivable Modular Messaging system

✔	Steps
	Complete a full restore to the Survivable Modular Messaging system using the backup of the primary system that was transferred to the FTP/SFTP server from the primary system location. For more information, see Restoring MSS data on page 76. ⚠ **CAUTION:** Do not reboot the MSS when instructed at the completion of the restore. Click **Return to Main** and continue with the following steps.
	On the MSS, change the IP addresses for the MSS and MASs. Change IP addresses to the IP addresses for the Survivable Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Revising MSS IP addresses on page 78.
	Change the PPP IP addresses for remote access to the PPP IP addresses recorded on the Survivable Modular Messaging planning form. To change the PPP IP addresses for remote access, complete the following steps: 1. From the MSS Messaging Administration menu, select **Security > PPP Configuration**. 2. In the **PPP IP field**, type the new PPP IP addresses. 3. Click **Save**. 4. Click **Return to Main**.
	Change the product alarm ID of the MSS to the product alarm ID assigned by the ART tool to the Survivable Modular Messaging system MSS. The MSS product alarm ID is recorded on the Survivable Modular Messaging planning form. Complete the following steps to change the product alarm ID: 1. From the MSS Messaging Administration menu, select **Alarming > Alarming Configuration**. 2. In the **Product ID** field, type the new product alarm ID. 3. Click **Save**. 4. Click **Return to Main**.
	Test alarm origination. For more information, see Testing alarming origination on page 80.

Table 5: Setting up the Survivable Modular Messaging system

✔	**Steps**
	Change the MSS backup destination from LAN backup to DVD backup. To change the backup destination, complete the following steps: 1. From the MSS Messaging Administration menu, select **Backup/Restore > Configure Remote Storage**. 2. From the pull down list in the **Backup Mode** field, select **DVD-RAM**. 3. Click **Save**. 4. Click **Return to Main**.
	Reboot the MSS.
	Connect the USB II drive to MAS 1.
	Restore the image of the primary system MAS 1 that is stored on the USB II drive to MAS 1 of the Survivable Modular Messaging system. For instructions about how to restore the image using Acronis Backup and recovery software, see Restoring the MAS image on page 73.
	In case of QSIG integration, verify that all the Dialogic cards in the system are running.
	Change the corporate network IP address for MAS1. Change the IP address to the corporate network IP address for MAS 1 of the Survivable Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Changing MAS Corporate IP addresses on page 81.
	Change the RAS IP addresses for MAS1. Change the RAS IP addresses to the RAS IP addresses for MAS 1 of the Survivable Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Changing MAS RAS IP addresses on page 82.
	Disable Mailbox Monitor, Message Waiting Indicator (MWI) and Call Me service. For more information, see Disabling Modular Messaging services on page 83.

Table 5: Setting up the Survivable Modular Messaging system

✔	Steps
	Change the product alarm ID of MAS1 to the product alarm ID assigned by the ART tool to the Survivable Modular Messaging system voice mail domain. Change the product alarm ID of each MAS in the voice mail domain. The voice mail domain product alarm ID is recorded on the Survivable Modular Messaging planning form. Complete the following steps to change the product alarm ID: 1. On the MAS desktop, double click **Voice Mail System Configuration**. 2. On the **Voice Mail System Configuration** window, double click **Serviceability**. 3. On the **Serviceabilty - Voice Mail Domain** popup, in the **Product identifier** field, enter the new product alarm ID. 4. Click **OK**. 5. Close the **Voice Mail System Configuration** window.
	Connect the USB drive and restore the image to each additional MAS and supplementary server in the system. Change the corporate network IP address after restoring each MAS. Change the IP address for each MAS to the corporate network IP address for the corresponding MAS on the Survivable Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Changing MAS Corporate IP addresses on page 81. Change the RAS IP addresses after restoring each MAS. Change the RAS IP addresses for each MAS to the RAS IP address assigned to the Survivable Modular Messaging MAS by the ART tool. For more information, see Changing MAS RAS IP addresses on page 82.

Table 5: Setting up the Survivable Modular Messaging system

✔	Steps
	Configure the PBX integration for MAS 1. Complete the following steps to change the integration IP address for systems with IP H323 integration: 1. On the **Voice Mail System Configuration** window, select **MAS1**. 2. Double-click **PBX Integration**. 3. On the **General** tab of the **PBX Integration** dialog, click the **IP** option button in the **Integration Type** list. 4. Click the **IP H.323** tab. 5. Change the **PBX IP** address to Corporate LAN. 6. Change the MAS1 IP address of the Survivable Modular Messaging system as recorded on the Survivable Modular Messaging planning form. This is the IP address that the MAS uses to connect to the corporate LAN. 7. Click **OK**. 8. Close the **Voice Mail System Configuration** window. **Note:** This step is not required for systems with QSIG integration. Complete the following steps to reconfigure the PBX integration for SIP integration: 1. On the **Voice Mail System Configuration** window, select **MAS1**. 2. Select **PBXs**. 3. Select PBX name. 4. Click the **SIP** tab. 5. Edit the **Address/FQDN** in the **Gateways** field and enter the FQDN or IP address of the appropriate SES. 6. Click **Ok**.
	Update the hosts file located at *C:\WINDOWS\system32\drivers\etc* to ensure that the correct IP addresses are used for both Avaya Modular Messaging Servers at the Survivable site.
	Reboot **MAS1**.
	Log in to the MAS at the Survivable site and run the FEDBSync tool located at *C:\Avaya_Support\Tools\FEDBSync*. Click **Execute**. Wait for event 1027 to appear in the Windows Event Viewer.

Table 5: Setting up the Survivable Modular Messaging system

✔	Steps
	Verify the Survivable Modular Messaging system integration. Do this by placing a test call to the Modular Messaging pilot number using the Trunk Access Code (TAC) created for the Survivable Modular Messaging system. The Survivable Modular Messaging system TAC is recorded on the Survivable Modular Messaging planning form.
	Give a copy of the Survivable Modular Messaging guide and completed Survivable Modular Messaging planning form to the customer.
	From the Survivable Modular Messaging MAS1 desktop, create a remote connection to MAS1 of the primary system.
	Place a copy of the Survivable Modular Messaging guide and Survivable Modular Messaging planning form in the SMM-Share$ folder.
	With the customer, review the procedure for moving service to the Survivable Modular Messaging system in the event of a failure of the primary system.

Configuring Survivable Modular Messaging system for the WebLM Server

Survivable Modular Messaging system with one master WebLM Server

To configure the master WebLM Server on a standard Survivable Modular Messaging system after installation of a Modular Messaging Release 5.2 system or upgrade to Modular Messaging system Release 5.2, perform the following steps:

1. Access the MAS of the primary Modular Messaging system and open the Voice Mail System Configuration.
2. In the **Voice Mail System Configuration** window, double-click the **Licensing** tab.
3. In the **WebLM URL** field, enter the WebLM Server URL of the master WebLM Server.

   Note:

   Ensure that the WebLM Server is accessible and has a valid license installed on it. If the master WebLM Server URL is not accessible or a valid license is not installed, the Modular Messaging system goes into License Error mode. If the problem is not corrected within 30 days, the Modular Messaging system enters into License Restricted mode.

4. After a few minutes, the primary Modular Messaging system enters into License Normal mode. Set the Survivable Modular Messaging system in the **Standing by** mode.

   Note:

   > To keep the Survivable Modular Messaging system updated, restore the backup from the primary MSS system on the Survivable MSS system periodically. Each time you perform the restore on the Survivable MSS system, set the Survivable Modular Messaging system in the **Standing by** mode. Repeat step 4 after every MSS restore on a Survivable Modular Messaging system.

Survivable Modular Messaging system with one master and two local WebLM Servers

To configure the master WebLM Server and the local WebLM Server on a standard Survivable Modular Messaging system after installation of a Modular Messaging Release 5.2 system or upgrade to Modular Messaging system Release 5.2, perform the following steps:

1. Set up the master WebLM Server and the two local WebLM Servers, one each for the primary Modular Messaging system and the Survivable Modular Messaging system.
2. From the master WebLM Server, push all the licenses to the primary local WebLM Server. For more information on pushing licenses, see the *Installing and Configuring Avaya WebLM Server* Guide.
3. Once the primary Modular Messaging system is up and running, access any MAS and open the Voice Mail System Configuration.
4. Double-click the **Licensing** tab.
5. Enter the WebLM Server URL of the primary local WebLM Server in the **WebLM URL** field.

   Note:

   > Make sure that primary local WebLM Server is accessible and has a valid license. If the primary local WebLM Server URL is not accessible or it does not have valid licenses, the primary Modular Messaging system enters into License Error mode. If you do not correct the problem within 30 days, the primary Modular Messaging system enters into License Restricted mode.

6. After ten minutes, the primary Modular Messaging system enters into License Normal mode. Access any MAS of the Survivable Modular Messaging system and open the Voice Mail System Configuration.
7. Double-click the **Licensing** tab
8. Enter the WebLM Server URL of the survivable local WebLM Server in the **WebLM URL** field.

Note:

When the survivable local WebLM Server does not have a license, the Survivable Modular Messaging system enters into License Error mode. After 30 days, the Survivable Modular Messaging system enters into License Restricted mode.

Switching service to the Survivable Modular Messaging system

Complete the steps in this checklist to switch service to the Survivable Modular Messaging system if the primary system fails.

All procedures described in this checklist are completed at the location of the Survivable Modular Messaging system or from a remote connection to that system.

Prerequisites

Before you can complete the procedures in this checklist, the following conditions must be met:

- The Survivable Modular Messaging system must be fully installed and configured. Steps described in Capturing primary Modular Messaging system information on page 26 and Setting up the Survivable Modular Messaging system on page 29 must be completed.

Additional requirements

To complete the procedures in this checklist, you must have the following:

- A copy of the Survivable Modular Messaging planning form with all information completed.

Checklist

Table 6: Switching service to the Survivable Modular Messaging system

✔	Steps
	On the Enterprise Survivable Server (ESS) or Local Survivable Processor (LSP) change the route pattern for Modular Messaging so that it routes calls to the Survivable Modular Messaging trunk group created in Setting up the Survivable Modular Messaging system on page 29. For more information, see Changing the Modular Messaging route pattern on page 84. The Modular Messaging route pattern number and Survivable Modular Messaging trunk group number are recorded on the Survivable Modular Messaging planning form.
	On the Survivable Modular Messaging system, enable Mailbox Monitor, Message Waiting Indicator (MWI) and Call Me services. After enabling services, verify that all required Modular Messaging services are running. For more information, see Enabling and starting Modular Messaging services on page 85.
	Enable DNS on the MSS. To enable DNS, complete the following steps: 1. From the MSS Messaging Administration menu, select **Server Administration > TCP/IP Network Configuration > Configure Network Addressing**. 2. In the **Enable DNS** field, select **Yes**. 3. Click **Save**.
	Verify voice mail service. To verify voice mail service, complete the following steps: 1. Place a test call to the Survivable Modular Messaging system by calling your extension. 2. Leave a message. 3. Verify that the Message Waiting Indicator is lit. 4. Retrieve the message. 5. Verify the call is integrated. For additional information, see *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration, Release 5, Installation and Upgrades.*

Table 6: Switching service to the Survivable Modular Messaging system

✔	**Steps**
	Arrange with the customer for an update of Fully Qualified Domain Name (FQDN) and IP address information on the customer's DNS server. DNS entries must be modified to point to the IP addresses assigned to the servers in the Survivable Modular Messaging system. This update is the customer's responsibility. See the Survivable Modular Messaging planning form for DNS server information.
	Test client access and subscriber options if applicable.
	Test web clients and WSO if applicable.
	If the primary Survivable Modular Messaging system is part of a messaging network, send a test message to and from the Survivable Messaging system from another Modular Messaging system on the network.
	Change the MSS backup destination from DVD backup to LAN backup to a location on the local Survivable Modular Messaging FTP/SFPT server. To change the backup destination, complete the following steps: 1. From the MSS Messaging Administration menu, select **Backup/Restore > Configure Remote Storage**. 2. In the Backup Mode field, select FTP or SFTP to specify the mode to use for the file backup to the remote location. 3. Complete or verify the fields on the page. Enter data for the FTP/SFTP server located at the Survivable Modular Messaging location. 4. Click **Save**. 5. When the system displays a message that the parameters have been saved, click **OK**. 6. Click **Test Connection** to validate the connection to the FTP server based on the page settings. 7. Click **Return to Main** to return to the Messaging Administration main menu. See *Administering remote storage for MSS backup* on the Modular Messaging, Release 5.2 documentation media for additional instructions about setting up MSS backup to the FTP or SFTP server.
	Arrange with the customer for a replication of the full MSS backup data from the primary Modular Messaging FTP/SFTP server to the one at the Survivable Modular Messaging location. For more information, see Restoring MSS data on page 76.

Making the Survivable Modular Messaging system as Active

Survivable Modular Messaging system with one master WebLM Server

After completing the steps in the checklist to switch service to the Survivable Modular Messaging system if the primary system fails, perform the following steps:

1. Access any MAS of the Survivable Modular Messaging system and open the Voice Mail System Configuration.
2. In the Voice Mail System Configuration window, double-click the **Licensing** tab.
3. Select the **Active** option to make the Survivable Modular Messaging system active. After ten minutes, the Survivable Modular Messaging system enters into License Normal mode.

   Note:

   > When the primary Modular Messaging system fails, the system automatically switches to the Survivable Modular Messaging system. The survivable mode changes to **Active Alarm** from **Standing by** because of an incoming call on the Survivable Modular Messaging system. To resolve the alarm, administrator should click the **Resolve Alarm** button in the **Licensing** tab in VMSC. If the administrator does not want to wait till the first call comes on the Survivable Modular Messaging system, administrator can change the survivable mode to **Active** when the primary Modular Messaging system fails.

Survivable Modular Messaging system with one master and two local WebLM Servers

After completing the steps in the checklist to switch service to the Survivable Modular Messaging system if the primary system fails, perform the following steps:

1. Go to the master WebLM Server.
2. Wait for the licenses to be released back to the WebLM Server. Licenses are automatically released after 10 minutes if they are not renewed.
3. Pull all the licenses from the primary local WebLM Server and push them to the survivable local WebLM Server. For more information on pushing licenses, see the *Installing and Configuring Avaya WebLM Server* Guide.
4. Access any MAS of the Survivable Modular Messaging system and open the Voice Mail System Configuration.
5. In the Voice Mail System Configuration window, double-click the **Licensing** tab. After ten minutes, the Survivable Modular Messaging system enters into License Normal mode.

Returning service to the primary Modular Messaging system

Complete the steps in this checklist to return service to the primary Modular Messaging system.

Procedures described in this checklist are completed at the locations of both the primary Modular Messaging system and the Survivable Modular Messaging system.

Note:

> If the MAS servers were left intact at the time of the primary system failure, it is not necessary to complete the steps in this procedure that restore the MAS servers. In this case it is necessary only to backup and restore the MSS and complete the switch administration described in the checklist.

Prerequisites

Before you can complete the procedures in this checklist, the following conditions must be met:

- To begin the procedure, the Survivable Modular Messaging system must be fully operational.
- Installation of the primary Modular Messaging system hardware including all physical LAN connections must be complete.

  Customer-provided servers in the primary Modular Messaging system must have the same host name as the corresponding server in the Survivable Modular Messaging system.
- Installation and configuration of additional servers for system functions that will not reside on an MAS or the supplementary server must be complete. For example, installation may include servers for the Web Client, Subscriber Options, or Web Subscriber Options if it does not reside on an MAS. These servers are not replicated as part of the instructions described in this manual. Follow normal installation procedures for these servers.
- Avaya recommends that you administer an announcement on the switch indicating that voice mail service is not available temporarily. Configure the switch to route calls to this announcement while the Modular Messaging system is out of service.

Additional requirements

To complete the procedures in this checklist, you must have the following:

- 300GB or larger USB II drive. After information has been captured from the Survivable Modular Messaging system, this drive must be shipped or hand carried to the location of the primary Modular Messaging system.

- A customer-provided copy of the software required to create a full bare-metal restore of the MASs and supplementary servers. One copy of the software is required for each server.
- The bootable rescue media DVDs that were created when the Survivable Modular Messaging system was installed. If you do not have these, for instructions about how to create these DVDs using Acronis Backup and recovery software, Creating bootable media on page 72
- A copy of the Survivable Modular Messaging planning form that was completed when the Survivable Modular Messaging system was installed. A copy of this form may be found in the SMM-Share$ folder on MAS1.
- A copy of the DCT data file created at the time of the installation of the primary Modular Messaging System. The DCT data file has the extension mmdct, such as sitefile.mmdct. You will need the DCT data file to configure the MSS and each MAS. See Selecting or creating a DCT data file on page 75.

Checklist

Table 7: Returning service to the primary Modular Messaging system

✔	Steps
	Connect the USB II drive to MAS1 of the Survivable Modular Messaging system.
	Create an image of MAS1 on the USB II drive. For instructions about how to create the image using Acronis Backup and recovery software, see Using Acronis Backup and recovery on page 72.
	Create an image of each additional MAS and supplementary server in the Survivable Modular Messaging system on the USB II drive.
	Detach the USB II drive and arrange with the customer for the drive to be transported to the primary Modular Messaging location. Alternately, you can arrange to carry the drive to the primary Modular Messaging location.
	Verify that the Survivable Modular Messaging MSS is set up for LAN back up. To verify LAN back up, complete the following steps: 1. Log on to the MSS. 2. From the MSS Messaging Administration menu, select **Backup/Restore > Configure Remote Storage**. 3. In the **Backup Mode** field, verify that FTP or SFTP is selected. See *Administering remote storage for MSS backup* on the Modular Messaging, Release 5.2 documentation media for additional instructions about setting up MSS backup to the FTP or SFTP server.

Table 7: Returning service to the primary Modular Messaging system

✔	Steps
	Conduct a full attended back up of the MSS. To conduct a backup, complete the following steps: 1. From the MSS Messaging Administration menu, select **Backup/Restore>Backup**. If you did not stop the messaging software before starting the backup, the system displays a warning message. Click **Continue Backup** to continue without stopping the messaging software, or click **Stop the Voice System** to exit the Backup page and stop the messaging software. 2. Select **yes** from the drop-down list for all data types to ensure a full backup. 3. Click **Start Backup**. 4. Click Continue after verifying information the system displays about the backup. 5. Verify that the system displays a message that the full backup has been successfully completed. 6. Click **Return to Main**. For more information, see *Performing an attended backup to a remote storage location* on the Modular Messaging, Release 5.2 documentation media for detailed instructions.
	Arrange with the customer for a replication of the full MSS backup data from the Survivable Modular Messaging FTP/SFTP server to the one at the primary Modular Messaging location.
	At the primary Modular Messaging system location, log on to the primary system MSS.
	Verify that the host name of the MSS matches the host name that was used by the Survivable Modular Messaging MSS. **Note:** The host names should be identical since the Survivable Modular Messaging MSS was initially configured with the primary system host name. To verify the name, complete the following steps: 1. From the MSS Messaging Administration menu, select **Server Administration > TCP/IP Administration > Configure Network Addressing**. 2. In the **Host Name** field, verify the name of the primary MSS. 3. If necessary edit the host name to match the name of the Survivable Modular Messaging system. See the Survivable Modular Messaging planning form for the name of the primary MSS.

Table 7: Returning service to the primary Modular Messaging system

✔	Steps
	Complete a full restore to the primary Modular Messaging system using the backup of the Survivable Modular Messaging system that was transferred to the FTP/SFTP server from the Survivable Modular Messaging system location. ⚠ **CAUTION:** Do not reboot the MSS when instructed at the completion of the restore. Click **Return to Main** and continue with the following steps.
	On the MSS, change the IP addresses for the MSS and MASs. Change IP addresses to the IP addresses for the primary Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Revising MSS IP addresses on page 78.
	Change the product alarm ID of the MSS to the product alarm ID of the primary Modular Messaging system MSS. Complete the following steps to change the product alarm ID: 1. From the MSS Messaging Administration menu, select **Alarming > Alarming Configuration**. 2. In the **Product ID** field, type the new product alarm ID. 3. Click **Save**. 4. Click **Return to Main**.
	Reboot the MSS.
	Connect the USB II drive to MAS1.
	Restore the image of the Survivable Modular Messaging system MAS1 that is stored on the USB II drive to MAS1 of the primary Modular Messaging system. For instructions about how to restore the image using Acronis Backup and recovery software, see Using Acronis Backup and recovery on page 72.
	Change the corporate network IP address for MAS1. Change the IP address to the corporate network IP address for MAS1 of the primary Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Changing MAS Corporate IP addresses on page 81.
	Change the RAS IP addresses for MAS1. Change the RAS IP addresses to the RAS IP addresses for MAS 1 of the primary Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Changing MAS RAS IP addresses on page 82.

Table 7: Returning service to the primary Modular Messaging system

✔	Steps
	Change the product alarm ID of MAS1 to the product alarm ID of the primary Modular Messaging system voice mail domain. Complete the following steps to change the product alarm ID: 1. On the MAS desktop, double click **Voice Mail System Configuration**. 2. On the **Voice Mail System Configuration** window, double click **Serviceability**. 3. On the **Serviceabilty - Voice Mail Domain** popup, in the **Product identifier** field, enter the new product alarm ID. 4. Click **OK**. 5. Close the **Voice Mail System Configuration** window.
	Connect the USB drive and restore the image to each additional MAS and supplementary server in the system. Change the corporate network IP address after restoring each MAS. Change the IP address for each MAS to the corporate network IP address for the corresponding MAS on the primary Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Changing MAS Corporate IP addresses on page 81. Change the RAS IP addresses after restoring each MAS. Change the RAS IP addresses for each MAS to the RAS IP address for the corresponding MAS on the primary Modular Messaging system. For more information, see Changing MAS RAS IP addresses on page 82. Change the product alarm ID after restoring each MAS following the procedure described in the preceding step. Change the product alarm ID for each MAS to the product alarm ID for the corresponding MAS on the primary Modular Messaging system.
	Verify the primary Modular Messaging system integration. Do this by placing a test call to the Modular Messaging pilot number using the Trunk Access Code (TAC) of the primary Modular Messaging system. If additional acceptance testing is required, see *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration, Release 5, Installation and Upgrades.*
	Stop calls to the Survivable Modular Messaging system. To stop calls, on the Enterprise Survivable Server (ESS) or Local Survivable Processor (LSP) administer Avaya Communication Manager to route Modular Messaging calls to an alternate location, such as an announcement.

Table 7: Returning service to the primary Modular Messaging system

✔	Steps
	On the Survivable Modular Messaging system, disable Mailbox Monitor, Message Waiting Indicator (MWI) and Call Me service. For more information, see Disabling Modular Messaging services on page 83.
	Stop the messaging service. To stop the messaging service, complete the following steps on the MSS: 1. Click **Utilities > Stop Messaging**. 2. On the **Stop Messaging Software** page, click **Stop**. The system displays a security warning about sending unencrypted information. 3. Click **Continue** 4. After the system reports that the voice system has completely stopped, click **Return to Main**.
	Conduct a second full attended back up of the Survivable Modular Messaging MSS to capture changes since the cutover procedure started. To conduct a backup, complete the following steps: 1. From the MSS Messaging Administration menu, select **Backup/Restore>Backup**. If you did not stop the messaging software before starting the backup, the system displays a warning message. Click **Continue Backup** to continue without stopping the messaging software, or click **Stop the Voice System** to exit the Backup page and stop the messaging software. 2. Select **yes** from the drop-down list for all data types to ensure a full backup. 3. Click **Start Backup**. 4. Click Continue after verifying information the system displays about the backup. 5. Verify that the system displays a message that the full backup has been successfully completed. 6. Click **Return to Main**. For more information, see *Performing an attended backup to a remote storage location* on the Modular Messaging, Release 5.2 documentation media for detailed instructions.

Table 7: Returning service to the primary Modular Messaging system

✔	**Steps**
	After completing the full backup, change the MSS backup destination from LAN backup to DVD backup. To change the backup destination, complete the following steps: 1. From the MSS Messaging Administration menu, select **Backup/Restore > Configure Remote Storage**. 2. From the pull down list in the **Backup Mode** field, select **DVD-RAM**. 3. Click **Save**. 4. Click **Return to Main**.
	Arrange with the customer for a replication of the full MSS backup data from the Survivable Modular Messaging FTP/SFTP server to the one at the primary Modular Messaging location.
	Log on to the primary system MSS.
	Complete a full restore to the primary Modular Messaging system using the most recent backup of the Survivable Modular Messaging system that was transferred to the FTP/SFTP server from the Survivable Modular Messaging system location. ⚠ **CAUTION:** Do not reboot the MSS when instructed at the completion of the restore. Click **Return to Main** and continue with the following steps.
	On the MSS, change the IP addresses for the MSS and MASs. Change IP addresses to the IP addresses for the primary Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Revising MSS IP addresses on page 78.
	Change the product alarm ID of the MSS to the product alarm ID of the primary Modular Messaging system MSS. Complete the following steps to change the product alarm ID: 1. From the MSS Messaging Administration menu, select **Basic System Administration > Alarming Administration**. 2. In the **Product ID** field, type the new product alarm ID. 3. Click **Save**. 4. Click **Return to Main**.
	Test alarm origination. For more information, see Testing alarming origination on page 80.
	Reboot the MAS1.

Table 7: Returning service to the primary Modular Messaging system

✔	Steps
	On the primary Avaya Communication Manager system, change the route pattern for Modular Messaging so that it routes calls to the primary Modular Messaging trunk group. For more information, see Changing the Modular Messaging route pattern on page 84.
	Arrange with the customer for an update of Fully Qualified Domain Name (FQDN) and IP address information on the customer's DNS server. DNS entries must be modified to point to the IP addresses assigned to the servers in the primary Modular Messaging system. This update is the customer's responsibility. See the Survivable Modular Messaging planning form for DNS server information.
	Test client access and subscriber options if applicable.
	Test web clients and WSO if applicable.
	If the primary Modular Messaging system is part of a messaging network, send a test message to and from the primary Modular Messaging system from another Modular Messaging system on the network.

Making the primary Modular Messaging system as Active

Survivable Modular Messaging system with one master WebLM Server

After completing the steps in the checklist to return service to the primary Modular Messaging system, perform the following steps:

1. Access any MAS of the Survivable Modular Messaging system and open the Voice Mail System Configuration.
2. In the Voice Mail System Configuration window, double-click the **Licensing** tab.
3. Select the **Standing by** option to make the Survivable Modular Messaging system into the survivable stand by mode.The Survivable Modular Messaging system enters into License Error mode.
4. Access any MAS of the primary Modular Messaging system and open the Voice Mail System Configuration.
5. Select the **Active** option to make the primary Modular Messaging system into the active mode. After 10 minutes the primary Modular Messaging system becomes active and enters the Licensing Normal mode.

Survivable Modular Messaging system with one master and two local WebLM Servers

After completing the steps in the checklist to return service to the primary Modular Messaging system, perform the following steps:

1. Bring the primary Modular Messaging system back in the working state.
2. Access any MAS of the Survivable Modular Messaging system and open the Voice Mail System Configuration.
3. Double-click the **Licensing** tab.
4. Select the **Standing by** option to make the Survivable Modular Messaging system into the survivable stand by mode.
5. Go to the master WebLM Server and pull all licenses from the survivable local WebLM Server and push them to the primary local WebLM Server. For more information on pushing licenses, see the *Installing and Configuring Avaya WebLM Server* Guide.
6. Once the licenses have moved from survivable local WebLM Server to the primary local WebLM Server, go to the Voice Mail System Configuration of the primary Modular Messaging system.
7. Change the survivable mode to **Active**. After ten minutes, the primary Modular Messaging system enters into License Normal mode.

   Note:

   > Since there are no licenses available on the survivable local WebLM Server, the survivable Modular Messaging system enters into License Error mode. After 30 days, the survivable Modular Messaging system enters into License Restricted mode.

Chapter 4: System maintenance checklist and requirements

This chapter contains the procedural checklist for maintaining the readiness of the Avaya Survivable Modular Messaging system. Refer to Chapter 3: Installation and cutover checklists on page 25 for the procedures required to install and cutover to the Survivable Modular Messaging system, and to return service to the primary system.

This chapter includes the following checklists:

- Restoring data to the Survivable Modular Messaging system on page 58.
- Trial failover procedure for Survivable Modular Messaging system on page 61

Overview

It is important that the Survivable Modular Messaging system be kept in a state where it is ready to take over service as quickly as possible in the event of a failure of the primary Modular Messaging system. For this reason, the following requirements must be met:

- Any software updates to the primary Modular Messaging system, must be replicated to the Survivable Modular Messaging system. This includes patches, service packs, and virus updates as well as any other software updates.
- Any changes to the primary Modular Messaging system that result from a service call, must be replicated to the Survivable Modular Messaging system. For example, a service call might result in registry changes.
- Frequent restores of data from the primary Modular Messaging system to the Survivable Modular Messaging system must be conducted. Avaya recommends that a full restore of data to the Survivable Modular Messaging system be conducted daily following the daily scheduled backup of the primary system MSS. Routine restore on a daily basis offers the highest degree of disaster preparedness.

  Failure to conduct a daily restore will result in a delay in bringing the Survivable Modular Messaging system into service since the restore would then need to be conducted as part of the procedure to failover to the Survivable Modular Messaging system.

  For more information about conducting a restore to the Survivable Modular Messaging system, see Restoring data to the Survivable Modular Messaging system on page 58.

To maintain readiness of the Survivable Modular Messaging system, maintenance alarms and procedures are treated with the same priority as those of the primary system. There are minor differences in the maintenance procedures for a Survivable Modular Messaging system. The following lists summarize procedures that are different for a Survivable Modular Messaging system as compared to a primary system. For a detailed description, see *Survivable Modular Messaging Offer Alarms and Procedures*. The document can be found on the Avaya Enterprise Portal under **Modular Messaging > Sales Collateral and Tools > Application Notes**. For more information about Modular Messaging maintenance, see *Monitoring and maintaining the system* on the Modular Messaging, Release 5.2 documentation media.

The following alarms require no action since the condition is considered normal for the Survivable Modular Messaging configuration:

- MT ALARM_ORIG 1
- VM LDAP-upd01
- VM LDAP-upd02
- VM LDAP-upd03
- VM NET_CON 0
- VM SERVER 900

- VM SERVER 901
- VM SOFTWARE 7715
- MT ABS_PROC 3
- MT ABS_PROC 5
- MT ALARM_ORIG 1

The following alarms require a different action for the Survivable Modular Messaging configuration as compared to the primary system:

- EL SHADOW 6
- VM MSGING_FS 2
- VS MAILBOX 1
- VS VOICE 3
- VS VOICE 4

Restoring data to the Survivable Modular Messaging system

Complete the steps in this checklist to routinely restore data to the Survivable Modular Messaging system from the primary Modular Messaging system.

All procedures described in this checklist are completed at the location of the Survivable Modular Messaging system or from a remote connection to that system.

Prerequisites

Before you can complete the procedures in this checklist, the following conditions must be met:

- The Survivable Modular Messaging system must be fully installed and tested. Procedures described in Capturing primary Modular Messaging system information on page 26 and Setting up the Survivable Modular Messaging system on page 29 must have been previously completed.
- The customer must have replicated the full backup of the primary MSS from the FTP/SFTP server at the primary Modular Messaging system location to the FTP/SFTP server at the Survivable Modular Messaging location.

  Avaya recommends that the system be set up to automatically replicate the full MSS backup to the FTP/SFTP server at the Survivable Modular Messaging location following the daily scheduled MSS backup.

Additional requirements

To complete the procedures in this checklist, you must have the following:

- A completed copy of the Survivable Modular Messaging planning form.
- A copy of the DCT data file created at the time of the installation of the primary Modular Messaging System. The DCT data file has the extension mmdct, such as sitefile.mmdct. You will need the DCT data file to configure the MSS and each MAS. See Selecting or creating a DCT data file on page 75.

Checklist

Table 8: Restoring data to the Survivable Modular Messaging system

✔	**Steps**
	Log on to the Survivable Modular Messaging MSS.
	Complete a full restore to the Survivable Modular Messaging system using the most recent full backup of the primary system that was transferred to the FTP/SFTP server from the primary system location. For more information, see Restoring MSS data on page 76. ⚠ **CAUTION:** Do not reboot the MSS when instructed at the completion of the restore. Click **Return to Main** and continue with the following steps.
	On the MSS, change the IP addresses for the MSS and MASs. Change IP addresses to the IP addresses for the Survivable Modular Messaging system as recorded on the Survivable Modular Messaging planning form. For more information, see Revising MSS IP addresses on page 78.
	Change the product alarm ID of the MSS to the product alarm ID assigned by the ART tool to the Survivable Modular Messaging system MSS. The MSS product alarm ID is recorded on the Survivable Modular Messaging planning form. Complete the following steps to change the product alarm ID: 1. From the MSS Messaging Administration menu, select **Alarming > Alarming Configuration**. 2. In the **Product ID** field, type the new product alarm ID. 3. Click **Save**. 4. Click **Return to Main**.
	Change the MSS backup destination from LAN backup to DVD backup. To change the backup destination, complete the following steps: 1. From the MSS Messaging Administration menu, select **Backup/Restore > Configure Remote Storage**. 2. From the pull down list in the **Backup Mode** field, select **DVD-RAM**. 3. Click **Save**. 4. Click **Return to Main**.

Table 8: Restoring data to the Survivable Modular Messaging system

✔	**Steps**
	Reboot the MSS and associated MAS.
	Copy caller applications to the Survivable Modular Messaging system whenever changes are made to the caller applications of the primary Modular Messaging system. If you create and deploy caller applications locally on the primary Modular Messaging system MAS, see Duplicating caller applications on page 86. If you create caller applications on an external PC, complete the following steps: 1. Copy the .uma file to the primary Modular Messaging system and deploy 2. Copy the same .uma file to the Survivable Modular Messaging system and deploy. For a detailed description of the steps required to deploy caller applications, see *Deploying Caller Applications to a VMD* on the Modular Messaging, Release 5.2 documentation media. **Note:** In either case, the .uma file must be identical on both the primary and Survivable Modular Messaging systems. Do not use a “save” or “save as” procedure to transfer the .uma file to the Survivable Modular Messaging system. Use the copy procedure described in this step or in Duplicating caller applications on page 86.

Trial failover procedure for Survivable Modular Messaging system

Failover refers to the process of switching the operations of a primary Modular Messaging system to the Survivable Modular Messaging system. You can do a trial failover to make sure that the failover procedures work in case of an actual failover. This section describes the trial failover steps.

Standard configuration

Standard configuration with one master WebLM Server

1. Take a backup of the primary Modular Messaging system and restore the backup on Survivable Modular Messaging system.
2. Shutdown all MAS of the primary Modular Messaging system, or stop the MM Message Application Server service on all the MASs of the primary Modular Messaging system.
3. On the Enterprise Survivable Server (ESS) or the Local Survivable Processor (LSP), change the route pattern for Modular Messaging so that it routes calls to the Survivable Modular Messaging trunk.
4. When the Survivable Modular Messaging system receives an incoming call, the mode changes from **Standing by** to **Active Alarm** mode. A major alarm is raised to notify the administrator that now the Survivable Modular Messaging system is handling the calls.

   Note:

   > Administrator can suppress this alarm to prevent the alarm from reaching the services by using **VMSC** > **Serviceability**.

5. Go to **VMSC** > **Licensing** tab of the Survivable Modular Messaging system.
6. Click **Resolve Alarm**. The mode of the Survivable Modular Messaging system changes from **Active Alarm** to **Active**.
7. After performing testing on the Survivable Modular Messaging system, bring the primary Modular Messaging system in working state.
8. Access any MAS of the Survivable Modular Messaging system and open the Voice Mail System Configuration.
9. On the **Licensing** tab, change the survivable mode from **Active** to **Standing By**.
10. On the Enterprise Survivable Server (ESS) or the Local Survivable Processor (LSP), change the route pattern for Modular Messaging so that it routes calls back to the Primary Modular Messaging trunk.

11. Access any MAS of the primary Modular Messaging system and open the Voice Mail System Configuration.
12. On the **Licensing** tab, change the survivable mode to **Active**. After 10 minutes the primary Modular Messaging system enters the License Normal mode and start handling the calls.

With one master WebLM Server and two local WebLM Servers

1. Take a backup of the primary Modular Messaging system and restore the backup on the Survivable Modular Messaging system.
2. Pull all the licenses from the primary local WebLM Server and push them to the survivable local WebLM Server.
   For more information on pushing licenses, see *Installing and Configuring Avaya WebLM Server* Guide.
3. On the Enterprise Survivable Server (ESS) or the Local Survivable Processor (LSP), change the route pattern for Modular Messaging so that it routes calls to the Survivable Modular Messaging trunk.
4. Shutdown all MAS of the primary Modular Messaging system, or stop the MM Message Application Server service on all the MASs of the primary Modular Messaging system.
5. When the Survivable Modular Messaging system receives an incoming call, the mode changes from **Standing by** to **Active Alarm**. A major alarm is raised to notify the administrator that now the Survivable Modular Messaging system is handling the calls.

   Note:

   > Administrator can suppress this alarm to prevent the alarm from reaching the services by using **VMSC** > **Serviceability**.
6. Go to **VMSC** > **Licensing** tab of the Survivable Modular Messaging system.
7. Click **Resolve Alarm**. The mode of the Survivable Modular Messaging system changes from **Active Alarm** to **Active**.
8. After performing testing on the Survivable Modular Messaging system, bring the primary Modular Messaging system in working state.
9. Go to the master WebLM Server and pull all the licenses from the survivable local WebLM Server and push them to the primary local WebLM Server.
   For more information on pushing licenses, see the *Installing and Configuring Avaya WebLM Server* Guide.
10. Access any MAS of the Survivable Modular Messaging system and open the Voice Mail System Configuration.
11. On the **Licensing** tab, change the survivable mode from **Active** to **Standing By**.

12. On the Enterprise Survivable Server (ESS) or the Local Survivable Processor (LSP), change the route pattern for Modular Messaging so that it routes calls back to the Primary Modular Messaging trunk.
13. Access any MAS of the primary Modular Messaging system and open the Voice Mail System Configuration.
14. On the **Licensing** tab, change the survivable mode to **Active**. After 10 minutes the primary Modular Messaging system enters the License Normal mode and start handling the calls.

Live configuration

Live configuration with one master WebLM Server

Perform step 2 to step 12 as described for a Standard configuration with one master WebLM Server.

Live configuration with one master WebLM Server and two local WebLM Servers

Perform step 2 to step 14 as described for a Standard configuration with one master WebLM Server and two local WebLM Servers.

Live configuration with periodic backup and restore

Live configuration with periodic backup and restore with one master WebLM Server

Perform all steps as described for a Standard configuration with one master WebLM Server.

Note:

Step 1 is optional.

Live configuration with periodic backup and restore with one master WebLM Server and two local WebLM Servers

Perform all steps as described for a Standard configuration with one master WebLM Server and two local WebLM Servers.

Note:

Step 1 is optional.

Chapter 5: Survivable Modular Messaging planning form

Table 9: Survivable Modular Messaging planning form

Primary Modular Messaging system corporate network IP address and DNS Information				
	DNS Fully Qualified Domain Name (FQDN)	Corporate Network IP Address	Subnet MASK IP Address	Gateway IP Address
MSS				
MAS1				
MAS2				
MAS3				
MAS4				
MAS5				
MAS6				
Web Client server				
WSO server				
CLAN IP (H.323 trunk, if applicable)				
CLAN IP (if applicable)				
Survivable Modular Messaging system corporate network IP address and DNS Information				
	DNS Fully Qualified Domain Name (FQDN)	Corporate Network IP Address	Subnet MASK IP Address	Gateway IP Address
MSS				
MAS1				
MAS2				
MAS3				
MAS4				
MAS5				

Table 9: Survivable Modular Messaging planning form

MAS6				
Web Client server				
WSO Server				
CLAN IP (if applicable)				
DNS IP addresses				
Server	IP address		Notes	
DNS 1				
DNS 2				
Survivable Modular Messaging FTP server information				
IP address				
Host name				
User				
Directory			Path to MSS backup on FTP server.	
Password				
Port				
Modular Messaging services				
Service	Location		Notes Enter server where services are running. For more information, see the primary system System Planning forms.	
MWI, Mailbox Monitor, and Call Me Service				
Product alarm IDs				
Primary system MSS product alarm ID				
Primary system MAS/VMD product alarm ID				
Survivable system MSS product alarm ID				
Survivable system MAS/VMD product alarm ID				
Call Routing Information				
		Number	Notes	

Table 9: Survivable Modular Messaging planning form

Route Pattern to be used for Survivable Modular Messaging		The primary system route pattern, which will be modified at cutover to route calls to the survivable system.
Survivable Modular Messaging trunk group number		Created during setup of survivable system.
Survivable Modular Messaging trunk access code (TAC)		Created during setup of survivable system.

RAS IP Addresses				
	Primary system RAS IP address 1	Primary system RAS IP address 2[1]	Survivable Modular Messaging System RAS IP address 1	Survivable Modular Messaging System RAS IP address 2[1]
MAS1				
MAS2				
MAS3				
MAS4				
MAS5				
MAS6				

[1] The second RAS IP address is determined by adding 1 to the RAS IP address assigned by the ART tool. Primary system RAS IP addresses can be found on the System Planning Forms created when the primary system was initially installed.

Chapter 6: Checklist procedures

This chapter contains detailed procedures for completing steps listed in the procedural checklists in Chapter 3: Installation and cutover checklists on page 25 and Chapter 4: System maintenance checklist and requirements on page 55. Only those steps requiring additional detail are described here. Procedures are listed in the order in which they first appear in the installation and cutover process. See the checklist you are using or the following list for a page number reference to the procedure you require.

The following procedures are described in this chapter:

- Validating FTP server communication on page 70
- Creating the SMM-Share$ folder on page 71.
- Using Acronis Backup and recovery on page 72
- Selecting or creating a DCT data file on page 75
- Restoring MSS data on page 76.
- Revising MSS IP addresses on page 78.
- Testing alarming origination on page 80.
- Changing MAS Corporate IP addresses on page 81.
- Changing MAS RAS IP addresses on page 82.
- Disabling Modular Messaging services on page 83.
- Changing the Modular Messaging route pattern on page 84.
- Enabling and starting Modular Messaging services on page 85.
- Duplicating caller applications on page 86.

Validating FTP server communication

Use this procedure to validate communication between the FTP server and the Survivable Modular Messaging system. This procedure must be completed prior to installation of the Survivable Modular Messaging system.

> ⚠ **CAUTION:**
>
> If the validation test fails, contact your support organization before proceeding with the installation.

To validate FTP server communication, complete the following steps:

1. Log in to any windows-based computer on the customer network. You can complete this test from an MAS or any windows-based PC.
2. On the desktop select **start > Run**.
3. In the **Open:** field, type **cmd** and click **OK**.
4. In the **cmd.exe** window, log in to the FTP server using the same credential that the MSS will use for backing up data to the FTP server.
5. Type **dir <*directory name*>**, where <*directory name*> is the directory that the MSS will use to back up data.
6. Verify that the window displays all the contents of the directory.

   > ⚠ **CAUTION:**
   >
   > If the dir command does not display the entire contents of the directory, then the validate test has failed. Contact your support organization before proceeding with the installation.

7. If the window displays the full contents of the directory, close the **cmd.exe** window and proceed with the installation of the Survivable Modular Messaging system.

For additional information, see the application note *Configuring Survivable Modular Messaging for Avaya Message Store using Avaya Enterprise Survivable Server*.

Creating the SMM-Share$ folder

This procedure is completed at the primary Modular Messaging system location as part of capturing the primary Modular Messaging system information.

To create the SMM-Share$ folder, complete the following steps:

1. Log on to MAS 1.
2. From the MAS desktop, open **My Documents**.
3. Right click on the **My Documents** window and select **New>Folder**.
4. Enter **SMM-Share$** for the folder name.
5. Right click on the folder and select **Sharing and Security**.
6. On the **SMM-Share$ Properties** window, click the **Share this folder** radio button.
7. Click Permissions.

   The **Permissions for SMM-Share$** window displays with **Everyone** highlighted.
8. On the **Permissions for SMM-Share$** window, click the **Allow** checkbox for **Full Control** for **Everyone**.

   The **Allow** checkboxes for **Change** and **Read** are automatically checked when **Full Control** is allowed. Verify that all three boxes are checked.
9. Click **OK** to close the **Permissions for SMM-Share$** window.
10. Click **OK** to close the **SMM-Share$ Properties** window.
11. Close the **My Documents** window.

    Note:

    > The SMM-Share$ folder is visible only in the account used to create it. Ensure that you use the login credentials of the customer who will manage the caller applications.

Using Acronis Backup and recovery

These procedures are completed at the primary location as part of capturing the primary Modular Messaging system information. Acronis Backup and recovery for Windows is used to create bootable media DVDs, which are in turn used to create backup images of the primary system MASs and supplementary servers. These bootable media DVDs are subsequently used to restore the backup images to the USB drive.

Creating bootable media

To create the bootable media DVDs, complete the following steps:

1. Install *Acronis Backup and recovery* on a standalone computer or any server.
2. Start the application. From the list of tools, select **Create Bootable Rescue Media**.
3. On the **Rescue Media Contents Selection** window, select **Acronis Backup and recovery version 10**.
4. Click **Next**.
5. Insert a blank DVD in the DVD drive.
6. On the **Bootable Media Selection** window, select **DVD-RW Drive**.
7. Click **Next** to complete the operation.
8. Label the DVD and save it for all backup and restore operations on windows machines.

Creating backup image of MAS 1

Creating a backup image of the MASs and the supplementary server enables you to restore the system in minutes in case of severe data damages or hardware failure.

Note:

> If the MAS that you are creating the backup image of has services such as MWI or Call me running, inform the customer that the services will be out for about an hour.

To create a backup image of MAS1 on the USB drive, complete the following steps:

1. Insert Acronis media in the DVD drive.
2. Connect the USB drive to the USB port on MAS1.
3. Restart MAS1.
4. Click **Acronis Backup and recovery version 10**.

5. On the **Acronis bootable Agent** window, select **Management Console.**
6. On the **Actions** tab, select **Backup**.
7. On the **Data to Backup** window, select the source disk which needs to be backed up.
8. Select **Backup sector-by-sector**.
9. Click **OK**.
10. On the **Where to backup** tab, in the **Archives** area, click **Change**.
11. Enter the destination path of the USB drive where backup is to be done.
12. Click **OK**.
13. Make sure that backup type is set to full on **How to backup** tab.
14. Click **OK** to start the backup.
15. After successful completion of backup, click **Close**.
16. Repeat steps 1 to 15 for each MAS and supplementary server.

Restoring the MAS image

To restore the backup from USB drive to MAS1, complete the following steps:

1. Connect the USB drive to MAS 1.
2. Insert Acronis media in the DVD drive.
3. Click **Acronis Backup and recovery version 10**.
4. On the **Acronis bootable Agent** window, select **Management Console.**
5. On the **Actions** tab, select **Recover**.
6. On the **What to recover** tab, in the **Archives** area, click **Change**.
7. On the **Backup Archive** selection window, select the file that you want to restore.
8. Click **OK**.
9. Select a data type.
10. If data type is set to **Disk**:
    a. Click **Change**.
    b. Select appropriate disk listed in the **Backup Contents** area.
    c. Click **OK**.
11. On the **Where to recover** tab, click **Change.**
12. Select the primary hard drive of the current system.
13. Click **OK**.

14. Set NT signature to **Keep Existing**.
15. Click **OK** to start the recovery.
16. Repeat steps 1 to 15 for each MAS and supplementary server.

Selecting or creating a DCT data file

If you have a Data Collection Tool (DCT) data file (*.mmdct) already created for installation at the primary site, be sure that it is accessible to the MAS that you are installing. In most cases this means inserting a USB storage device with the file into a USB port 1 on the S3500, S8730, S8800 1U, or HP DL360 G7 server prior to starting the system. If you do not have a data file already created, you will be able to create one during the installation when completing step 4 of this procedure.

Complete the following steps to configure the MAS from the DCT data file:

1. Verify that the USB storage device with the DCT data file and most recent DCT executable file is inserted in the USB port.
2. When the Modular Messaging Configuration Wizard (MMCW) launches, the Modular Messaging Welcome screen is displayed. Click Next.
3. If you have a DCT data file already created for this installation, complete the following steps and proceed to step 5. If you don’t have a DCT data file, go to step 4.
    a. On the **Locate Configuration Data** screen, highlight the DCT data file for this installation. If the file is not displayed, click **Browse** and browse to the directory where the file is stored. By default, the MMCW searches the hard drive for all files with the file type *.mmdct.
    b. After selecting the DCT data file that was created for this installation, click **Next**. You are prompted to verify the file selection. Click **Yes** to select the file.
    c. On the last screen, click **Complete** and then save the file again if you have made any changes.
    d. Proceed to Step 5.
4. If you must create a DCT data file from completed planning forms, complete the following steps.
    a. On the **Locate Configuration Data** screen, check the box to **Create a new configuration file**. Click **Next**.
    b. When the system prompts you to create a new configuration file, click **Yes**. The DCT executable file launches.
    c. Use the information in the Planning forms to enter data for each screen. As you progress through the pages, a green check mark indicates screens with complete and valid information. A red x indicates screens with incomplete or invalid data.
    d. On the last screen, click **Complete** and then save the file.
5. Click **Complete** to continue.

Restoring MSS data

Use this procedure to restore backed up data from the FTP/SFTP server at the primary or Survivable Modular Messaging location to the MSS. Use the procedure in the following cases:

- When setting up the Survivable Modular Messaging system.

  When setting up a new Survivable Modular Messaging system, use this procedure to duplicate information from the primary system to the Survivable Modular Messaging system.

- After a routine backup and restore to the Survivable Modular Messaging system.

  When routinely updating backup information to the Survivable Modular Messaging system, use this procedure to duplicate information from the primary system to the Survivable Modular Messaging system.

- When returning service to the primary system use this procedure to duplicate information from the Survivable Modular Messaging system to the primary system.

To restore the data you must first change the system backup procedure to retrieve information from a remote storage location (FTP/SFTP server). You must then restore the data.

To restore data, complete the following steps:

1. From the MSS Messaging Administration menu, select **Backup/Restore** > **Configure Remote Storage**.

   The system displays the Configure Remote Storage page.

2. In the Backup Mode field, select FTP or SFTP to specify the mode to use for the file backup to the remote location.

   The system displays the fields required for the backup mode you selected.

3. Complete the fields on the page. For more information about this web-based administration page, click the field names or **Help**.

   - When restoring information to the Survivable Modular Messaging system, enter data for the FTP/SFTP server located at the Survivable Modular Messaging location. This information is recorded on the Survivable Modular Messaging planning form.

   - When returning service to the primary Modular Messaging system, enter data for the FTP/SFTP server located at the primary Modular Messaging location.

If you selected FTP in the Backup Mode field, proceed to step 6. If you selected SFTP in the Backup Mode field, if it has not already been done, you must generate the public cryptographic key to be used for authentication between the MSS and the remote SFTP server:

4. Click **Regenerate RSA public key**. The system displays the generated key in the RSA public cryptographic key window.

5. Transfer the public key to the customer's SFTP server. One way to do this is to copy the text from the cryptographic key window to a file, paste the key into a file, transfer the file to the

remote SFTP server, and then paste the key into the appropriate file on the remote SFTP server. The file to which you must copy the public key information depends on the SFTP version being used on the remote server. For example, for SSH1 use the $HOME/.ssh/authorized_keys or $HOME/.ssh/authorized_key2 file.

Note:

> After you generate the initial public key, you should not need to regenerate the public key unless it is a customer security requirement.

6. Click **Save**.

   The system displays a message that the parameters have been saved.
7. Click **OK**.
8. Click **Test Connection** to validate the connection to the FTP server based on the page settings.
9. Click **Return to Main** to return to the Messaging Administration main menu.
10. From the Messaging Administration main menu, select **Backup/Restore>Restore**.

    The system displays a message that proceeding with the restore will overwrite existing data.
11. Click **Proceed with Restore** to continue.

    The system displays the View/Restore Contents of FTP/SFTP Server page.
12. Select the backup data to restore. Check all data types to ensure a full restore.
13. Click **Start Restore** to restore the data from the selected backup.
14. Do not reboot the system at this time. Return to the checklist to continue.

For additional information about conducting and verifying a restore, see *Restoring backed-up MSS data* on the Modular Messaging, Release 5.2, documentation media.

Revising MSS IP addresses

Use this procedure to change the IP addresses of the MSS, MASs and supplementary servers as they are recorded on the MSS. Use the procedure in the following cases:

- When setting up the Survivable Modular Messaging system.

  When setting up a new Survivable Modular Messaging system, the restore procedure transfers the IP addresses of the primary system to the survivable system. Use this procedure to replace the primary system IP addresses with information unique to the Survivable Modular Messaging system.

- After a routine backup and restore to the Survivable Modular Messaging system.

  Each time the Survivable Modular Messaging system is updated with a new backup and restore, its IP addresses are overwritten with the primary system IP addresses. These IP addresses must be replaced with the IP addresses unique to the Survivable Modular Messaging system.

- When returning service to the primary system.

  When returning service to the primary system, the IP addresses transferred from the Survivable Modular Messaging system must be changed to the IP addresses originally assigned to the primary system.

To change the IP addresses, complete the following steps:

1. From the MSS Messaging Administration menu, select **Server Administration > TCP/IP Network Configuration > Configure Network Addressing**.
2. In the Default Gateway Address field, type the MSS default gateway address recorded on the Survivable Modular Messaging planning form.
3. In the IP Address field, type the MSS IP address recorded on the Survivable Modular Messaging planning form.
4. In the **Enable DNS** field, select **No**.
5. Click **Save**.
6. Click the browser **Back** button.
7. Click **MAS Host Setup**.
8. In the **MAS ID field**, select MAS1. Click **Edit**.
9. In the **Public IP Address** field, type the IP address for MAS1 recorded on the Survivable Modular Messaging planning form.
10. Click **Save**.
11. Click **Back**.
12. Repeat Steps 8 through 11 for each additional MAS and supplementary server in the system.

⚠ **CAUTION:**

If you fail to change the MSS public IP address, you can not browse to the server using the corporate IP address. However, you could still use Remote Desktop Connection to log in to the MAS and then use the private IP address of the MSS to log in from the MAS browser window.

Testing alarming origination

Use this procedure when setting up the Survivable Modular Messaging system or when returning service to the primary system to verify that alarms are logged correctly and are sent to the correct destination.

Note:

This test requires that the receiving system, either INADS or SNMP, is set up and ready to receive alarms.

To test alarm origination:

1. From the Messaging Administration main menu, click **Diagnostics** > **Alarm Origination**.

   The system displays the Test Alarm Origination page.

2. To test alarm origination screen, click **Run Test**.
3. If the alarm origination test must use the modem, log off as quickly as possible.
4. Wait 5 minutes for the test alarm to be acknowledged and resolved.
5. Access the Alarm Log. You can either:
   - Click **Display Alarm Log** from the Test Alarm Origination page.
   - From the Messaging Administration main menu, click **Logs** > **Alarm Log**.

   The system displays the Alarm Log page.

6. Click **Display** to determine if the minor alarm VM type ALARM_ORIG is still active. If so:
   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,* the maintenance process **MAINT** resolves the alarm in 30 minutes. If this happens, check the administration to verify that you have a good connection to the remote service center. Correct any settings, and then retry this test.

Changing MAS Corporate IP addresses

Use this procedure to change the corporate network IP addresses of the MASs and supplementary servers. Use the procedure in the following cases:

- When setting up the Survivable Modular Messaging system.

  When setting up a new Survivable Modular Messaging system, the restore procedure transfers the IP addresses of the primary system to the survivable system. Use this procedure to replace the primary system corporate network IP addresses with Survivable Modular Messaging corporate network IP addresses on each MAS and supplementary server.

- When returning service to the primary system.

  When returning service to the primary system, the IP addresses transferred from the Survivable Modular Messaging system must be changed to the IP addresses originally assigned to the primary system.

To change the corporate network IP addresses, complete the following steps:

1. On the MAS desktop, right click **My Network Places**. Select **Properties**.
2. On the **Network Connections** window, double click **Corporate LAN**.
3. On the **Corporate LAN Status** pop up, click **Properties**.
4. On the **Corporate LAN Properties** pop up, highlight **Internet Protocol(TCP/IP)** and click **Properties**.
5. On the **Internet Protocol (TCP/IP) Properties** popup, in the **IP address** field, enter the new IP address.
6. In the **Default Gateway** field enter default gateway information for the Survivable Modular Messaging system.
7. Click **Advanced**.
8. On the **Advanced TCP/IP Setting** popup, select the **DNS** tab and verify that the **Register this connection's addresses in DNS** checkbox is NOT checked.
9. Click **OK** to exit the Advanced TCP/IP popup.
10. Click **OK** to change the IP address and exit the **Internet Protocol (TCP/IP) Properties** pop up.
11. Click **OK** to close the **Corporate LAN Properties** pop up.
12. Close the **Corporate LAN Status** pop up and **Network Connections** window.

Changing MAS RAS IP addresses

Use this procedure to change the RAS IP addresses of the MASs and supplementary servers. Use the procedure in the following cases:

- When setting up the Survivable Modular Messaging system.

  When setting up a new Survivable Modular Messaging system, the restore procedure transfers the IP addresses of the primary system to the survivable system. Use this procedure to replace the primary system RAS IP addresses with the Survivable Modular Messaging RAS IP addresses assigned by the ART tool to each MAS and supplementary server.

- When returning service to the primary system.

  When returning service to the primary system, the RAS IP addresses transferred from the Survivable Modular Messaging system must be changed to the RAS IP addresses originally assigned to the primary system.

To change the RAS IP addresses, complete the following steps:

1. Double-click the **Configure** icon on the desktop
2. In the left pane of the **Configure** window, expand **Routing and Remote Access**.
3. Right-click the server name and select **Properties**
4. In the local **Properties** window for the server, click the **IP** tab.
5. Under **IP address assignment**, select **Static address pool**.
6. Select the displayed IP address range and click **Edit**.
7. In the Address Range window, enter the correct start and end IP addresses for this server. See the Survivable Modular Messaging planning form for the correct addresses.
8. Verify that the number of addresses is 2.
9. Click **OK**
10. Click **OK** again to close the **Properties** window.
11. Close the **Configure** window.

Disabling Modular Messaging services

Use this procedure to disable Mailbox Monitor, Message Waiting Indicator and Call Me services on the Survivable Modular Messaging system when it is not in use. Use this procedure under the following circumstances:

- When setting up the Survivable Modular Messaging system.
- After a routine backup and restore of primary system information to the Survivable Modular Messaging system.

To disable Modular Messaging services, complete the following steps:

1. On the MAS desktop, double click the **Monitor** icon.
2. Click **Services (Local)** in the left pane, if the item is not already selected.
3. In the right pane of the Monitor window, scroll down to **MM Call Me Server**.
4. Double-click the service to open the **Properties** window.
5. Set the **Startup type** to **Disabled**.
6. Click **OK**.
7. Repeat steps 3 through 6 for **MM Message Waiting Indicator Server** and **MM Mailbox Monitor** (in that order).
8. Refresh the screen and verify that all three services are **Disabled**.
9. Close the **Monitor** window.

Changing the Modular Messaging route pattern

Use this procedure to change the route pattern used to route calls from the Avaya Communication Manager server to the Modular Messaging system.

Use this procedure in the following cases:

- When switching service from the primary Modular Message system to the Survivable Modular Messaging system after failure of the primary system.
- When returning service to the primary Modular Messaging system.

To change the Modular Messaging route pattern, complete the following steps:

1. Log on to Avaya Communication Manager.
   - When switching service to the Survivable Modular Messaging system, log on to the Enterprise Survivable Server (ESS) or Local Survivable Processor (LSP) at the Survivable Modular Messaging location.
   - When returning service to the primary Modular Messaging system, log on to the primary Avaya Communication Manager system.
2. Enter the command **change route-pattern <route number>**, where route number is the number of the pattern used to route calls to the Modular Messaging system.
3. On the **change route-pattern** screen, under the **Grp No** column, in row 1, type the number of the trunk group that will now be used for the Modular Messaging system.
   - When switching service to the Survivable Modular Messaging system, change the **Grp No** to the number of the trunk group that routes calls to the Survivable Modular Messaging system.
   - When returning service to the primary Modular Messaging system, change the **Grp No** to the number of the trunk group that routes calls to the primary Modular Messaging system.

   Note:

   If multiple trunk groups are used for Modular Messaging, change all relevant trunk group numbers.
4. Save the change and exit the screen.

Enabling and starting Modular Messaging services

Use this procedure to enable Mailbox Monitor, Message Waiting Indicator and Call Me services on the Modular Messaging MAS that will host these services. Also use it to verify the status of all Modular Messaging services. Use this procedure under the following circumstances:

- When switching service to the Survivable Modular Messaging system after the primary system has failed.
- When returning service to the primary Modular Messaging system.

To enable Modular Messaging services, complete the following steps:

1. On the MAS desktop, double click the **Monitor** icon.
2. Click **Services (Local)** in the left pane, if the item is not already selected.
3. In the right pane of the Monitor window, scroll down to **MM Mailbox Monitor.**
4. Double-click the service to open the **Properties** window.
5. Set the **Startup type** to **Automatic**.
6. Under **Service status**, click **Start**.
7. Click **OK**.
8. Repeat steps 4 through 7 for **MM Message Waiting Indicator Server** and **MM Call Me Server** (in that order).
9. Refresh the screen and verify that all three services are set to **Automatic**.
10. Verify that all Modular Messaging services required for this MAS are started:
    a. Scroll to the list of Modular Messaging services. These services start with the letters 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 types of **Automatic**.
       - Services that are not required for this server must show a blank status and a startup type of **Disabled**. See Disabling Modular Messaging services on page 83 for more information about disabling services.

         If necessary, consult the System Planning form for the primary system to determine which services reside on each server.

    b. To start a service with a startup type of Automatic, right click the service and select **Start**.
11. Close the **Monitor** window.

Duplicating caller applications

Use this procedure to copy caller applications to the Survivable Modular Messaging system if caller applications are usually deployed on an MAS in the primary Modular Message system. If caller applications are usually deployed on an external PC, see the procedure described in Restoring data to the Survivable Modular Messaging system on page 58.

Copy caller applications to the Survivable Modular Messaging system whenever changes are made to the caller applications of the primary Modular Messaging system.

Always save the caller applications for your primary Modular Messaging system in the SMM-Share$ folder on MAS1. This folder was created as part of setting up the Survivable Modular Messaging system. For more information, see Capturing primary Modular Messaging system information on page 26 and Creating the SMM-Share$ folder on page 71.

To copy caller applications to the Survivable Modular Messaging system, complete the following steps:

1. On MAS1 of the primary Modular Messaging system, open **MASx**. In this release the **My Computer** icon on the desktop is automatically renamed to the name of the MAS based on the information provided in the DCT file during installation.
2. Navigate to the **SMM-Share$** folder for the primary system MAS.
3. Open a second occurrence of **MASx**.
4. Navigate to the SMM-Share$ folder of the Survivable Modular Messaging system. If you have not previously mapped a drive to this folder, complete the following steps.
   a. On the **MASx** window, select **Tools>Map Network Drive**.
   b. From the **Drive** pull-down menu, select a drive letter.
   c. In the **Folder** field enter **\\<*ip address*>\SMM-Share$**, where **<*ip address*>** is the ip address of MAS1 of the Survivable Modular Messaging system.
   d. Click **Finish**.
5. Drag and drop the .uma file from the SMM-Share$ folder of the primary system to the SMM-Share$ folder of the Survivable Modular Messaging system.
6. Log on to MAS1 of the Survivable Modular Messaging system.
7. Open the .uma file in the Survivable Modular Messaging SMM-Share$ folder and deploy the caller applications. For a detailed description of the steps required to deploy caller applications, see *Deploying Caller Applications to a VMD* on the Modular Messaging, Release 5.2 documentation media.