



Message Networking Help

[Home](#) | [Search](#)
[Print](#) | [Back](#) | [Fwd](#) | [Close](#)
[Getting Started](#)
[Administration](#)
[Installation](#)
[Maintenance](#)
[Reference](#)
[Home](#) > [Reference](#) > [Print Guides](#) > Concepts and Features print guide

Concepts and Features print guide

This print guide is a collection of Message Networking Help system topics provided in an easy-to-print format for your convenience. Please note that the links shown in this document do not work online, and that some of the topics link to tasks that are not included in the PDF file. The online system contains all Message Networking documentation and is your primary source of information.

This printable guide contains the following topics:

Topic	Page Number
Message Networking concepts and features	2
What's new in Message Networking Release 5.2	3
Message Networking features	6
Message Networking network configurations	8
Server descriptions	13
Attended high-availability option overview	25
Supported networking types	28
Supported remote machine types	33
Remote machine overview	35
Message Networking subscribers	84
Enterprise Lists overview	91
Simple Network Management Protocol overview	96
Message Networking language support	101
Bridging feature overview	103
Overview of MultiSite for Message Networking	107
Overview of Avaya Aura™ Messaging for Message Networking	110
LDAP overview	113
Message Networking system capacities	116
Administrator interface	120
Message Networking maintenance	121
System security	122





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > Message Networking concepts and features



Message Networking concepts and features

Message Networking allows networking customers to simplify their network topology and administration by supporting store-and-forward message protocols. With Message Networking, you can exchange messages between [supported multimedia messaging systems](#).

This topic provides general information about Message Networking:

- [What's new in Message Networking Release 5.2](#)
- [Message Networking features](#)
- [Message Networking network configurations](#)
- [Server descriptions](#)
- [Attended high-availability configuration](#)
- [Supported networking types](#)
- [Supported remote machine types](#)
- [Remote machines overview](#)
- [Message Networking subscribers overview](#)
- [Enterprise List overview](#)
- [SNMP overview](#)
- [Message Networking language support](#)
- [Bridging feature overview](#)
- [MultiSite overview](#)
- [LDAP overview](#)
- [Message Networking system capacities](#)
- [Message Networking message component types](#)
- [Administrator interface](#)
- [Message Networking maintenance](#)
- [System security](#)

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > What's new in Message Networking Release 5.2



What's new in Message Networking Release 5.2

In addition to the many features and capabilities provided in previous releases, Avaya Message Networking Release 5.2 offers the following new or enhanced features and capabilities:

- [Security enhancements](#)
- [Support for S8800 2U hardware](#)
- [Support for S3500 Basic hardware](#)
- [Support for MultiSite enabled Modular Messaging remote machine](#)
- [Support for Avaya Aura™ Messaging](#)
- [Support for variable length mailboxes in MultiSite enabled Modular Messaging remote machines](#)
- [Support for 2nd Nature for Messaging Multisite remote systems](#)
- [System installation and administration improvements](#)
- [SPIRIT for remote serviceability](#)
- [SAL remote access mechanism](#)

Security enhancements

The following security enhancements have been added to Message Networking for Release 5.2:

- [Stringent password rules](#)
- [Message exchange using standard SMTP, secure SMTP, or both](#)
- [File transfer using HTTPS/SSL encryption](#)
- [AAA LDAP plain password encryption](#)

Stringent password rules

To improve control over access to the Message Networking system, an administrator operating in an appropriate role can now specify more stringent password rules to the group of locally-authenticated system accounts.

Message exchange using standard SMTP, secure SMTP, or both

The Message Networking allows exchange of messages to and from other remote systems that support secure SMTP. The Message Networking allows you to use standard SMTP, secure SMTP, or both with the secure socket layer (SSL) encryption.

File transfer using HTTPS/SSL encryption

The Message Networking ensures secure file transfer from and to the Message Networking server. The Message Networking provides menus from the Message Networking administration interface for the secure file transfer.

AAA LDAP plain password encryption

AAA LDAP server supports encrypting the login credentials in plain text. The encrypted password is stored in .aaaconfig.ldappwd file. New installs for the basic offer are supported on the S3210R and S3500 Basic server.

Support for S8800 2U hardware

Avaya introduces S8800 2U servers for Message Networking from Release 5.2. All new installations of Message Networking Release 5.2 can be performed on the S8800 2U server. Existing Message Networking systems may continue to use the S3500-H or S3210R server, or can migrate to the S8800 2U server.

Support for S3500 Basic hardware

Avaya introduces S3500 Basic servers for Message Networking from Release 5.2. All new installations of Message Networking Release 5.2 can be performed on the S3500 Basic server. Existing Message Networking systems may continue to use the S3500-H or S3210R or S8800 2U server. The S3210R systems can migrate to the S3500 Basic server.

Support for MultiSite enabled Modular Messaging remote machine

Message Networking now supports connecting to a MultiSite enabled Modular Messaging systems with Message Networking. MultiSite enabled Modular Messaging systems can have mailbox numbers of variable lengths. Message Networking voice networks with network addresses of a fixed length of up to 10 digits will now support mailbox numbers of variable lengths from 3 - 30 digits from a MultiSite enabled Modular Messaging systems.

Support for Avaya Aura™ Messaging

Avaya Aura™ Messaging, also referred as Messaging, is the next generation messaging product from Avaya. Messaging is designed for enterprises with complex data and telephony environments. Messaging is flexible, scalable, resilient, and easy to deploy on standard Linux based servers.

Support for variable length mailboxes in MultiSite enabled Modular Messaging and Avaya Aura™ Messaging remote machines

For Modular Messaging MultiSite and Avaya Aura™ Messaging remote machines, the Message Networking system can be administered to accept messages from subscribers who have different length mailbox numbers. For example, subscribers on the same remote machine could have mailbox numbers (also called mailbox IDs) that have four digits and five digits on a single Modular Messaging MultiSite and Avaya Aura™ Messaging remote machines. In previous releases, all mailbox numbers for these remote machines had to have the same number of digits.

Support for 2nd Nature for Messaging Multisite and Avaya Aura™ Messaging remote systems

Message Networking supports Unimax 2nd Nature (2N) and supports changes for Messaging Multisite and Avaya Aura™ Messaging systems.

System installation and administration improvements

The following improvements are included in this release:

- A pre-upgrade tool produces a report that your software specialist uses to plan an upgrade from Message Networking R1.1, R2.0 or R3.1 systems. This tool is installed on the Message Networking system before an upgrade or migration.
- A backup verification tool analyzes the backup media. This tool is installed on the Message Networking system before an upgrade or migration.

SPIRIT for remote serviceability

The Message Networking hardware platform includes SPIRIT, a serviceability agent that autonomously raises an alarm if a processor fails or if environmental problems occur. All Message Networking systems are installed with SPIRIT, which provides remote serviceability using IP access. SPIRIT replaces the older modem-access agents, including Avaya Serviceability Agent. Avaya also offers SAC (Secure Access and Control)-Lite and SAC-Premium, which provides serviceability access using VPN.

The Message Networking system can be configured to send alarm notifications to a service organization using SPIRIT or SNMP traps.

The Message Networking now provides the following alarming options using SPIRIT:

- **Modem Dialout**, modem based alarming
- **Internet**, HTTPS based alarming sent through the SPIRIT to the Avaya HTTPS servers
- **SNMP**, IP-based alarming with traps sent to the destinations of type INADS
 - **OAM** (To a customer's Network Management System)
 - **INADS** (Using an SSG (Avaya Secure Services Gateway) to forward alarms to Avaya Services)

SAL remote access mechanism

New installations, upgrade and migrations to Message Networking Release 5.2 support SAL remote access mechanism. The Message Networking system can be configured to send alarm notifications to a service organization using SAL. If you are administering alarm management via SAL, use the SAL Destinations page to administer SAL Gateways. INADS and OAM NMSs are administered on the SAL Gateway.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Message Networking features



Message Networking features

Message Networking features include:

- Support for multiple [network configurations](#), including hub and spoke, bridge, and hybrid. The bridge and hybrid configurations take advantage of Message Networking's [bridging feature](#).
- Support for MultiSite enabled Modular Messaging remote machines. For an overview on MultiSite, see [Modular Messaging MultiSite](#). For information on concepts and features of MultiSite, see *Modular Messaging MultiSite Guide*.
- Support for [S3210R](#), [S3500-H](#), [S8800 2U](#), and [S3500 Basic servers](#), to maximize flexibility.
- Support for a number of [networking types](#) and [remote machine types](#).
- Support for Unimax 2nd Nature for Messaging Multisite remote systems.
- Transport and protocol conversion that automatically transcodes message formats between all supported networking protocols.
- Message Networking-to-Message Networking and **Message Networking-to-Interchange 5.4 configurations** to increase network capacities.
- Directory views that allow a subset of names and subscriber remote pages to be downloaded from the Message Networking system to a specific location.
- [Variable-length numeric addressing](#) from Modular Messaging MultiSite and Avaya Aura™ Messaging systems.
- [Dial Plan Mapping](#), which allows you to map existing mailbox addresses to unique network addresses.
- Enterprise Lists that are created using a unique virtual mailbox on the Message Networking system to which subscribers can forward multimedia messages. This mailbox has a voice name and ASCII list name that can be administered. Messages can be addressed by list number or list ASCII name. **On** receipt of a list message, the system checks the appropriate permissions for use of the list. **Once the system verifies the permissions**, the Message Network sends the message to all recipients defined in the list. For information on administering Avaya Enterprise Lists, see [Elist Administration](#).
- Simple Network Management Protocol (SNMP) support that allows you to consolidate network management of all Message Networking machines using a TCP/IP LAN or WAN. For information on administering, see [SNMP Administration](#).
- Secure Access Link (SAL) is an Avaya serviceability solution for support and remote management of a variety of devices and products. SAL provides remote access and alarm reception capabilities. SAL uses the existing Internet connectivity of a customer to facilitate remote support from Avaya.
- Support for the following alarming options using SPIRIT:
 - **Modem Dialout**, modem based alarming
 - **Internet**, HTTPS based alarming sent through the SPIRIT to the Avaya HTTPS servers
 - **SNMP**, IP-based alarming with traps sent to the destinations of type INADS
 - **OAM** (To a customer's Network Management System)
 - **INADS** (Using an SSG (Avaya Secure Services Gateway) to forward alarms to Avaya Services).
- [Call Detail Recording](#) (CDR) **creates a message history and thus** helps manage message networks that use Message Networking. The history file includes: the status of the message, the source and destination of the message, and the time the **message enters and leaves** the Message Networking

system. This history file can be transferred from the Message Networking system to another system for reporting purposes using the FTP process.

- The ability to set the preferred language for announcements on a remote machine and subscriber basis. For more information, see [Message Networking language support](#).
- [LDAP interface](#) support, which allows you to perform queries and system administration and maintenance **through** an LDAP client.
- Role-Based Access Control (RBAC), which gives customers the ability to create administration accounts based on customer-defined roles. When you set up an administrative role, you specify which Web-administration pages the role can access and the access type. For more information, see [Role-Based Access Control](#) and [Managing administrative roles](#).
- Support for an Authentication, Authorization, and Accounting (AAA) sever. An AAA server is an optional, customer-provided server that can be used to authenticate administration accounts (logins) on the Message Networking system. For information about configuring the Message Networking system for login authentication by an AAA server, see [Configuring the system for login authentication by an AAA server](#).
- [System log reports](#) provide information about how the system is used, including data about features, subscribers, communities, data port loads, and remote messaging traffic, and which record events that are useful for maintaining the system, for diagnosing problems and troubleshooting the system, and for spotting trends or estimating future needs.
- The ability to send administrative logging information to an external, customer-provided server using the syslog protocol (RFC 3164). This is in addition to logging this information locally on the Message Networking server. For more information, see [Administering the system to send logging messages to an external server](#).
- [Attended and unattended system backups](#).
- The ability to set stringent password rules to improve control over access to the Message Networking system.
- Message exchange using standard SMTP on a default TCP/IP port 25, secure SMTP on a default TCP/IP port 465, or both standard and secure SMTP on a custom port.
- Support for encrypting AAA LDAP login credentials in plain text.
- [File Transfer Protocol \(FTP\) support](#) that allows the Message Networking report exports and subscriber imports.
- Secure file transfer support that allows [importing](#) and [exporting](#) of files from and to the Message Networking server using HTTPS/SSL.
- The ability to back up and restore system data through the use of a remote storage location on the customer LAN. You can use File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) to transfer system data to the remote storage location. For more information, see [Administering a remote storage location](#).
- Access to the sa login to create new administration accounts for logging in to the system either from the console or from another computer on the customer LAN. This login is in addition to the administration accounts that are available after the system is installed. For more information, see [Managing local administration accounts](#).
- Avaya Aura™ Messaging, also referred as Messaging, is the next generation messaging product from Avaya. Messaging is designed for enterprises with complex data and telephony environments. Messaging is flexible, scalable, resilient, and easy to deploy on standard Linux based servers. Messaging is an enterprise-class messaging system targeted for flexible deployment options, such as single site, multisite, centralized, and distributed. Messaging includes a suite of applications designed to increase productivity, responsiveness, and collaboration.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Message Networking network configurations



Message Networking network configurations

This topic provides information on the types of network configurations supported for Message Networking and general network configuration considerations.

Supported network configurations

Message Networking supports the following network configurations. See [Sample network topologies](#) for illustrations of the network topologies discussed in this topic.

- **Hub-and-spoke topology:** In this configuration, each system is only networked to the Message Networking system, which provides the conversion between the various protocols. Every system in the network can be networked to every other system using any of the protocols supported by Message Networking.

The **Number of Bridged Machines** option on the **Customer Options** page must be set to 500 (the maximum).

- **Bridge topology:** Message Networking supports a bridge network topology, in which Message Networking provides the network protocol conversion that allows a single remote machine or multiple remote machines to communicate with the rest of the systems in the network. In this scenario, Message Networking is normally not processing messages between the other systems in the network, but is dedicated to providing communication from the new systems to the existing network systems. A bridge topology is useful in a situation where new systems purchased support protocols not supported by the other systems in the network. A bridge topology can take the following forms:
 - A Message Networking system is used for each new system that is being bridged. While this topology is more costly because it requires a dedicated Message Networking system for each system as a bridge to the other networked systems, it provides greater network reliability as there is no single point of failure.
 - One Message Networking system is shared among multiple bridged machines.

To use a bridge topology, the **Number of Bridged Machines** option on the **Customer Options** page is set to the number of remote machines each Message Networking system is bridging, and each new system must be administered as a bridged system on the appropriate Message Networking system. For example, if you want to add three new systems to your existing network, and you purchase a Message Networking system to act as a bridge between the new systems and your existing network, then the **Number of Bridged Machines** must be set to 3 on the Message Networking system and you must administer each new system as a bridged system on the Message Networking system.

Sample bridge network configurations are provided on the Avaya support Web site. Go to <http://www.avaya.com/support> and then navigate to the Message Networking page.

- **Hybrid topology:** Message Networking supports a hybrid network topology, in which a combination of point-to-point, hub-and-spoke, or bridging exists within the same network. A hybrid network topology usually involves multiple Message Networking systems.

General network configuration considerations

The following general network configuration considerations apply to Message Networking:

- **Analog fallback:** Octel 250/350 and Octel 200/300 systems that are networked digitally in a point-to-point configuration have the ability to fall back to Octel Analog if the system is unable to send the message over the TCP/IP data network. Message Networking does not support this fallback either in an inbound (that is, messages from an Octel 250/350 or Octel 200/300) or an outbound direction. Although analog fallback does not occur on the Message Networking system when the TCP/IP network is unavailable, messages are rescheduled for delivery (based upon predefined delivery schedules), and no messages are lost. As more redundancies continue to be built into TCP/IP networks at the data level and these networks become more reliable, the need for analog fallback to be built at the application level becomes less of a requirement. This is true much in the same way that many other data applications, such as email, PC client access to message mailboxes, do not depend on analog fallback at the application level.
- **Uniform Network Address length:** Message Networking supports a uniform Network Address length from 3 to 10 digits. In some configurations, a prefix can be used when defining a dial plan. A prefix is a number that is dialed by the sender of a message before entering the digits of the Network Address (for example, dialing a 1 before a 10-digit Network Address). The prefix 1 is not actually transmitted to the Message Networking system along with the Network Address. In some networks, prefix use can give the appearance to the sender that the address lengths are variable but, in reality, the same number of digits is always transmitted to the Message Networking system for the Network Address. Message Networking does support variable-length addressing for Modular Messaging and Avaya Aura™ Messaging systems. For additional information on variable-length addressing, see [Administering numeric address mapping](#).
- **Multiple-length mailbox IDs:** Except for Serenade Octel Analog, Serenade Digital, and Modular Messaging MultiSite remote machines, Message Networking does not support multiple mailbox ID lengths within the same remote machine (message server). Each remote machine can have a different mailbox ID length, but the length of mailbox IDs cannot vary within a given remote machine. For Serenade Octel Analog, Serenade Digital, and Modular Messaging MultiSite remote machines, the Message Networking system can be administered to map multiple mailbox ID lengths to the uniform Network Address length.
- **Multiple Message Networking systems in a network:** In a network that includes multiple Message Networking systems, a message cannot traverse more than two Message Networking systems during a delivery. Each Message Networking system must be administered on every other Message Networking system in the same network.
- **Hybrid networks:** Message Networking supports hybrid network configurations in which there is a mix of point-to-point and Message Networking message server connections. It is important to be careful in planning the dial plan of such a network to ensure that the desired delivery path is followed when subscribers use the network. One issue that can occur in a hybrid network is "double name-back." This is a condition in which a subscriber has two paths to send a network message to a recipient: one as a direct point-to-point connection and another through the Message Networking system. When this occurs, two remote subscriber directory entries can be stored on the local message server: one for the point-to-point path and another for the Message Networking path. In this case, senders using the dial-by-name feature can get back two responses for the same person (for example, "Press 1 for John Smith, Press 2 for John Smith"). This condition can be prevented by defining one dial plan path by which a sender can send a message to a recipient.
- **Upgrading from Octel Analog to Digital:** Message Networking does not support the ability to change the connection type for a message server networked using Octel Analog to Aria Digital or Serenade Digital. These machines must be deleted from the Message Networking database and readministered as Aria Digital or Serenade Digital. Subscriber lists stored on the message servers can be impacted when the remote machine is deleted and then readministered.
- **Moving from a point-to-point configuration to Message Networking:** Note the following considerations when moving from a point-to-point configuration to Message Networking:
 - The dial plan can change such that lists stored on local message servers can be impacted. This impact might require that a user re-enter the list with the new Message Networking network address. Octel 250/350 servers support the ability to move a prefix from one remote machine to another (that is, from a remote machine connected point-to-point to a Message Networking system). When this is done, the lists that reference subscribers on the moved remote node remain unchanged.
 - The deletion of remote subscribers when moving from a point-to-point to a Message Networking

topology also causes the inability to use the INTUITY AUDIX Personal Address Book feature (Message Manager) to identify and address any deleted remote subscribers. Other related mailbox features that are affected include the Personal Directory (Touchtone User Interface Options 5, 2) and Names Directory (Touchtone User Interface Option **6, when addressing a message). Local INTUITY AUDIX subscribers would need to replace any deleted remote subscribers in their Personal Directory. The Personal Address Book and Names Directory are re-created when messaging remote subscribers through Message Networking. The Message Networking dynamic updates feature adds these to the local messaging system one-by-one on a real-time basis as messaging occurs between the systems.

- Message header information is lost permanently for old or saved messages stored in a subscriber's mailbox that were received from remote subscribers who were later deleted (as a result of moving from a point-to-point configuration to Message Networking). Saved messages in this case lose their header information and indicate a message from an unknown subscriber. In addition, end users do not have the ability to reply to messages from the deleted subscriber. The customer should be alerted to this condition prior to the conversion to the Message Networking network. Subscribers should take note of important saved messages and be prepared for this situation. In addition, unnecessary saved messages should be deleted before the Message Networking conversion.
- For Octel Analog, non-LDAP-based SMTP (VPIM and MIME), and AMIS remote machines, there are several possible methods of adding remote subscribers into the Message Networking system. The following is a list of these methods in order of preference:
 1. Bulk add by file
 2. Self-registration
 3. Sending a message through the Message Networking system (This method is not supported for an AMIS remote machine)
 4. Subscriber Parameters page
 5. Demand remote update (Octel Analog)
 6. Bulk add by range

Note: The bulk add by range utility is lowest on the preference list. While this method is a viable option, it should only be used when the other methods cannot be used. If you plan to use this utility, take note of the following considerations:

- When using bulk add by range, the administrator should limit the range administered on the Message Networking system to the actual range (or sub ranges) used on the remote message server. Otherwise it is possible for tens of thousands of default subscribers to be added for remote machines that actually only have a few hundred subscribers. Having thousands of unused default subscribers can impact system performance.
- Since Aria Digital and Serenade Digital systems support a demand NameSend and INTUITY AUDIX and Avaya Modular Messaging systems support Demand Remote Update to initialize the Message Networking subscriber database, a bulk add by range should never be used for these machine types (nor should any of the other add methods listed above). Additionally, the digital system types notify Message Networking when a new subscriber is added so that the Message Networking system can update its directory. In all cases, customers are encouraged to upgrade to a digital connection as the directory updates and administrative procedures for digital systems are much more robust than those for analog systems.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)[Back](#) | [Fwd](#) | [Close](#)[Getting Started](#)[Administration](#)[Installation](#)[Maintenance](#)[Reference](#)[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Sample network topologies

Sample network topologies

The following diagrams provide samples of the network topologies supported by Message Networking:

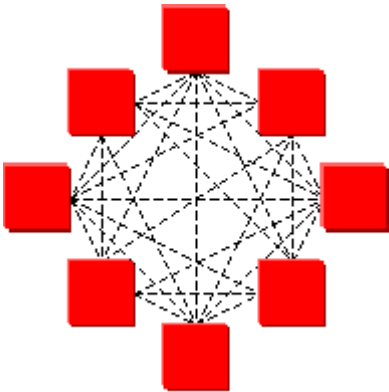
Point-to-point: This sample is provided to illustrate the complexity of the connections required when Message Networking is not present.

Hub-and-spoke: This sample illustrates a network where Modular Messaging and systems and other message systems are networked via a Message Networking system.

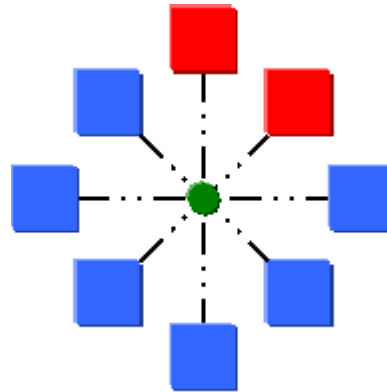
Bridge: This sample illustrates a network where bridging is used to connect Modular Messaging systems to an existing network.

Meshed hub-and-spoke: This sample illustrates a network where multiple Message Networking systems and Interchange 5.4 systems are used to connect messaging systems.

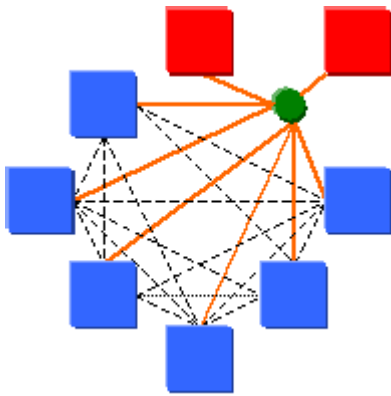
Point-to-point



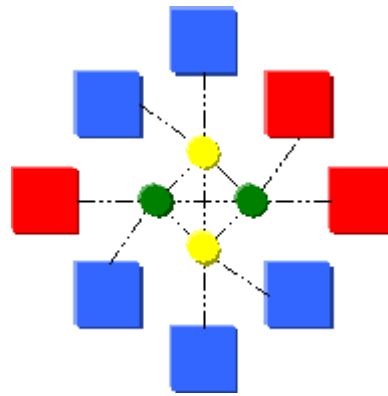
Hub-and-spoke










Bridge topology



Meshed hub-and-spoke



The following key provides an explanation of the diagrams.

	Modular Messaging
	Other Messaging
	Interchange
	Message Networking on S3210R, S8800 2U or S3500 Basic
	Point-to-point via common protocol
	Bridged via optimum protocol (traffic must be to/from bridged nodes)
	Hubbed via optimum protocol (traffic can be to/from any node)

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Server descriptions



Server descriptions

Message Networking supports the following servers:

- [S3210R](#)
- [S3500-H](#)
- [S3500 Basic](#)
- For information on S8800 2U, see [Maintaining the Avaya S8800 Server](#) guide (pdf).

The following table provides a high-level overview of the components in each server.

<

Component	S3210R	S3500-H	S8800 2U	S3500 Basic
Chassis	PCI	PCI	PCI	PCI
Slots available for port boards	3	1	2 PCIx, 1 PCIe	3
Rack-mountable	Yes	Yes	Yes	Yes
CPU	2.0 GHz Celeron	3.4 GHz Pentium IV with 1M L2 Cache	2.26 GHz Intel E5520 quad core	3.4 GHz Pentium IV with 1M L2 Cache
RAM	512 MB	2 GB	4 GB	2 GB
Max analog ports	12	For the 4-port analog board, the maximum is 4. For the 12-port analog board, the maximum is 12.	For the 4-port analog board, the maximum is 4. For the 12-port analog board, the maximum is 12.	3 4-port cards
Disk drive	1 IDE, 40 GB	Four 73 GB, 15,000 RPM, SCA SCSI hard disk drives	Three 146GB hard disk drives	1 80 GB IDE
CD/DVD	DVD-RW	DVD-RAM	DVD-RAM	DVD-ROM
RMB	No	Yes	No	No
Data redundancy	No	Yes (RAID Level 5), Ultra 320 PCI SCSI RAID card	Yes (RAID Level 5), P400 256 MB DDR-2 RAM controller with battery backed write cache (RAID card)	No
Power supply	90-264V AC,	90-250V AC, 47-63 Hz (redundant)	90-250V AC, 47-63	90-250V AC, 47-63 Hz

	47/63 Hz	and hot swappable)	Hz (redundant and hot swappable)	
Serial ports	2	2	1	2
Parallel ports	1	1	0	1
USB ports	4 at the back, 2 on the front	3 at the back, 1 on the front	2 at the back, 2 on the front	3 at the back, 1 on the front
LAN	One 10/100 Ethernet port	One 10/100/1000 Ethernet port and one 10/100 Ethernet port. Only the 10/100/1000 port is used; the 10/100 connector is capped.	2 ports of 1 GBPS	One 10/100/1000 Ethernet port and one 10/100 Ethernet port. Only the 10/100/1000 port is used; the 10/100 connector is capped.
Fan	2	4 (redundant and hot swappable)	3 (redundant and hot swappable)	4 (redundant and hot swappable)

Notes:

- New installations of Message Networking Release 5.2 are only supported on an S8800 2U, S3210R and S3500 Basic server.
- You can either upgrade Message Networking Release 3.1 that runs on S3500-H or S3210R servers to Message Networking Release 5.2 or migrate to Message Networking Release 5.2 that runs on S8800 2U and S3500 Basic server.

See [Comparison of Message Networking Release 5.2 servers](#) to help you determine which Message Networking Release 5.2 server best suits your needs.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Server description](#) > S3210R server



S3210R server

This topic provides information about the Message Networking S3210R server, which includes the following components:

- [Chassis](#)
- [Capacities](#)
- [Processor](#)
- [Voice/fax ports](#)
- [Storage devices](#)
- [Controllers](#)
- [Ports](#)
- [Monitor, keyboard, and mouse](#)
- [Modems](#)
- [Uninterruptible power supply](#)
- [Terminals](#)
- [Operating system](#)

Chassis

The S3210R server contains three PCI slots in a rack-mount or stackable configuration and two cooling fans.

Capacities

The Message Networking system with an S3210R server supports 500,000 subscribers (250,000 with voice names), 500 remote machines (with an average of 8 to 10), and 12 analog ports.

Note: Modular Messaging and Avaya Aura™ Messaging systems do not accept more than 250,000 subscribers (with or without voice names) during an update. Therefore, if the Message Networking system has more than 250,000 subscribers and you are updating to Modular Messaging and Avaya Aura™ Messaging remote machines, you must [administer the Modular Messaging remote machines](#) and [Avaya Aura™ Messaging remote machines](#) to use directory view updates. The [directory view](#) you administer for the Modular Messaging and Avaya Aura™ Messaging systems must include not more than 250,000 subscribers.

Processor

The server CPU is a 2 GHz processor and is equipped with 512 MB of RAM.

Voice/fax ports

Up to three 4-port analog port boards are supported to provide up to 12 ports of AMIS or Octel Analog Networking.

Storage devices

The server is equipped with an IDE hard drive and a DVD-RW drive, which is used for software installation and backups.

A portion of the hard disk is reserved for the storage of nonspeech data, such as data for the Linux operating system, the Message Networking system server executables and data, and the Message Networking system software executables. This disk area is important for proper Message Networking system operations and cannot be changed or used for any other purposes.

The rest of the hard disk is used for storing messaging components such as voice messages.

Controllers

The video, LAN, and IDE controllers reside on the motherboard.

Ports

The S3210R server contains a single parallel port, two serial ports, six USB ports, and one 10/100 Ethernet port.

Monitor, keyboard, and mouse

A monitor, keyboard, and mouse are required for local system operation. A monitor is available for purchase for use with the Message Networking system. Depending on your location, the keyboard and mouse are provided with the system. Contact your sales representative for more information.

Modems

Access for remote diagnostics is provided through an external modem. A serial modem is provided with the Message Networking system. A USB modem is also supported and is available for purchase. Contact your sales representative for more information.

Uninterruptible Power Supply

An Uninterruptible Power Supply (UPS) is strongly recommended for use with Message Networking systems.

Terminals

While it is recommended that you use the Web interface to administer the Message Networking system, you can also administer the system remotely through the use of a modem and one of the following terminals:

- Avaya 4410 (for PROCOMM PLUS 4410 or Terranova emulation)
- Avaya 715
- Avaya 4425
- vt100 (for vt100 or vt131 emulation)

Operating system

Linux is the operating system used for Message Networking. Linux is a UNIX-like operating system that runs on a variety of servers.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Server description](#) > S3500-H server



S3500-H server

This topic provides information about the Message Networking S3500-H server.

The S3500-H server includes the following components:

- [Chassis](#)
- [Capacities](#)
- [Processor](#)
- [Voice/fax ports](#)
- [Storage devices](#)
- [Controllers](#)
- [Ports](#)
- [Remote maintenance board](#)
- [Monitor, keyboard, and mouse](#)
- [Modems](#)
- [Uninterruptible power supply](#)
- [Terminals](#)
- [Operating system](#)

Chassis

The chassis is equipped with four cooling fans. In the chassis, the removable PCI card cage has a three-slot riser card.

Capacities

The Message Networking system with an S3500-H server supports 500,000 subscribers (250,000 with voice names), 500 remote machines (with an average of 25), and 12 analog ports.

If Enterprise Lists are being used, the maximum of 500,000 subscribers (250,000 with voice names) includes Enterprise Lists and any voice names for Enterprise Lists.

Note: Modular Messaging and Avaya Aura™ Messaging systems do not accept more than 250,000 subscribers (with or without voice names) during an update. Therefore, if the Message Networking system has more than 250,000 subscribers and you are updating to a Modular Messaging and Avaya Aura™ Messaging remote machines, you must [administer the Modular Messaging remote machines](#) and [Avaya Aura™ Messaging remote machines](#) to use directory view updates. The [directory view](#) you administer for the Modular Messaging and Avaya Aura™ Messaging system must include not more than 250,000 subscribers.

Processor

The server CPU is a 3.4 GHz Pentium IV processor and is equipped with 2 GB of RAM.

Voice/fax ports

The S3500-H supports either the 4-port or 12-port analog boards. A maximum of one analog port board is supported to provide up to 4 ports (with one 4-port board) or 12 ports (with one 12-port board) of AMIS or Octel Analog Networking.

A maximum of 4 fax ports are supported for simultaneous use on the 12-port board. Fax channels are assigned dynamically when fax is detected on an incoming call and when an outgoing call includes a fax component. If all four fax channels are in use simultaneously, retries might be experienced.

Storage devices

The server is equipped with four SCSI disks, with hardware RAID Level 5 data redundancy and a DVD-RAM drive, which is used for software installation and backups.

A portion of the hard disk is reserved for the storage of nonspeech data, such as data for the Linux operating system, the Message Networking system server executables and data, and the Message Networking system software executables. This disk area is important for proper Message Networking system operations and cannot be changed or used for any other purposes.

The rest of the hard disk is used for storing messaging components such as voice messages.

Controllers

The video and LAN controllers reside on the motherboard.

Ports

The server contains the following ports:

- Parallel port: 1
- Serial ports: 2
- USB ports: 3 at the back, 1 in front
- Ethernet ports: One 10/100/1000 Ethernet port and one 10/100 Ethernet port. Only the 10/100/1000 port is used, the 10/100 connector is capped.

Remote maintenance board

A remote maintenance board is provided to facilitate remote diagnostics and repair.

Note: For international Message Networking systems, an external modem is required to support the RMB.

Monitor, keyboard, and mouse

A monitor, keyboard, and mouse are required for local system operation. A monitor is available for purchase for use with the Message Networking system. Depending on your location, the keyboard and mouse are provided with the system. Contact your sales representative for more information.

Modems

For domestic U.S. systems, the RMB uses an internal modem. For systems outside the U.S., an external modem is required.

Uninterruptible Power Supply

An Uninterruptible Power Supply (UPS) with 30-minute holdover is required for the S3500-H server.

Terminals

While it is recommended that you use the Web interface to administer the Message Networking system, you can also administer the system remotely through the use of a modem and one of the following terminals:

- Avaya 4410 (for PROCOMM PLUS 4410 or Terranova emulation)
- Avaya 715
- Avaya 4425
- vt100 (for vt100 or vt131 emulation)

Operating system

Linux is the operating system used for Message Networking. Linux is a UNIX-like operating system that runs on a variety of servers.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Server description](#) > S3500 Basic server



S3500 Basic server

This topic provides information about the Message Networking S3500 Basic server, which includes the following components:

- [Chassis](#)
- [Capacities](#)
- [Processor](#)
- [Voice/fax ports](#)
- [Storage devices](#)
- [Controllers](#)
- [Ports](#)
- [Monitor, keyboard, and mouse](#)
- [Modems](#)
- [Uninterruptible power supply](#)
- [Terminals](#)
- [Operating system](#)

Chassis

The S3500 Basic server chassis is equipped with four cooling fans. In the chassis, the removable PCI card cage has a three-slot riser card.

Capacities

The Message Networking system with an S3500 Basic server supports 500,000 subscribers (250,000 with voice names), 500 remote machines (with an average of 8 to 10), and 12 analog ports.

Note: Modular Messaging and Avaya Aura™ Messaging systems do not accept more than 250,000 subscribers (with or without voice names) during an update. Therefore, if the Message Networking system has more than 250,000 subscribers and you are updating to the Modular Messaging and Avaya Aura™ Messaging remote machines, you must [administer the Modular Messaging remote machines](#) and [Avaya Aura™ Messaging remote machines](#) to use directory view updates. The [directory view](#) you administer for the Modular Messaging and Avaya Aura™ Messaging systems must include not more than 250,000 subscribers.

Processor

The server CPU is a 3.2 GHz Pentium IV processor and is equipped with 2 GB of RAM.

Voice/fax ports

Up to three 4-port analog port boards are supported to provide up to 12 ports of AMIS or Octel Analog Networking.

Storage devices

The server is equipped with an IDE hard drive for software installation and DVD-ROM.

A portion of the hard disk is reserved for the storage of nonspeech data, such as data for the Linux operating system, the Message Networking system server executables and data, and the Message Networking system software executables. This disk area is important for proper Message Networking system operations and cannot be changed or used for any other purposes.

The rest of the hard disk is used for storing messaging components such as voice messages.

Controllers

The video, LAN, and IDE controllers reside on the motherboard.

Ports

The S3500 Basic server contains the following ports:

- Parallel port: 1
- Serial port: 2
- USB port: 3 at the back, 1 in the front.
- Ethernet port: One 10/100/1000 Ethernet port and one 10/100 Ethernet port. Only the 10/100/1000 port is used, the 10/100 connector is capped.

Monitor, keyboard, and mouse

A monitor, keyboard, and mouse are required for local system operation. A monitor is available for purchase for use with the Message Networking system. Depending on your location, the keyboard and mouse are provided with the system. Contact your sales representative for more information.

Modems

Access for remote diagnostics is provided through an external modem. A serial modem is provided with the Message Networking system. A USB modem is also supported and is available for purchase. Contact your sales representative for more information.

Uninterruptible Power Supply

An Uninterruptible Power Supply (UPS) is strongly recommended for use with Message Networking systems.

Terminals

While it is recommended that you use the Web interface to administer the Message Networking system, you can also administer the system remotely through the use of a modem and one of the following terminals:

- Avaya 4410 (for PROCOMM PLUS 4410 or Terranova emulation)
- Avaya 715
- Avaya 4425
- vt100 (for vt100 or vt131 emulation)

Operating system

Linux is the operating system used for Message Networking. Linux is a UNIX-like operating system that runs on a variety of servers.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Installation](#) > [Upgrading to Message Networking Release 5.2](#) > Comparison of Message Networking Release 5.2 servers

Comparison of Message Networking servers

The following table provides a comparison of the Message Networking servers. This table is helpful when determining which Message Networking Release 5.2 server best suits your needs.

For more information on server components and supported features, see [Server description](#) and [Verifying customer options](#).

I need...	S8800	S3500-H	S3210R	S3500 Basic
Very high capacity message throughput	X	X		
Low-cost bridging solution			X	X
Enterprise Lists	X	X		
SNMP	X	X	X	X
Web browser-based administration	X	X	X	X
Analog protocols (Octel Analog Networking, AMIS)	X	X	X	X
Digital protocols (AUDIX TCP/IP, Aria TCP/IP, Serenade TCP/IP, VPIM, SMTP/MIME) Note: When referring to digital communication, the number of ports supported refers to the simultaneous TCP/IP sessions supported. For example, support for 12 SMTP ports indicates that the system supports a maximum of 12 simultaneous sessions shared by the SMTP/MIME and VPIM protocols. All digital communication on the Message Networking system is supported by the installed LAN card/connector.	X	X	X	X
Maximum number of analog ports (12) Support for analog ports is provided through analog port boards installed in the server and connected to the PBX. Note: The S3210R and S3500 Basic servers support a maximum of three 4-port analog boards, the S8800 supports one 4-port analog board or one 12-port analog board, and the S3500-H supports one 4-port analog board or one 12-port analog board.	X	X	X	X
SMTP/MIME Email connectivity	X	X	X	X
Can be administered by customers (test connect tools, and so on)	X	X	X	X
CDR	X	X		
FTP	X	X	X	X
LDAP	X	X	X	X
Rack-mount	X	X	X	X
Higher availability (RAID Level 5 hot swap disks, hot swap redundant fans, hot swap redundant power supply, UPS, and so on)	X	X		
Reports	X	X	X	X

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)[Back](#) | [Fwd](#) | [Close](#)[Getting Started](#)[Administration](#)[Installation](#)[Maintenance](#)[Reference](#)[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Attended high-availability option overview

Attended high-availability option overview

Message Networking Release 5.2 supports an attended high-availability option, which is intended for extreme disaster recovery circumstances when an operational Message Networking cannot perform normal operations due to unscheduled downtime.

The high-availability option is supported for the S3500-H and S8800 servers. The S3500-H and S8800 server provides additional reliability and availability features, including:

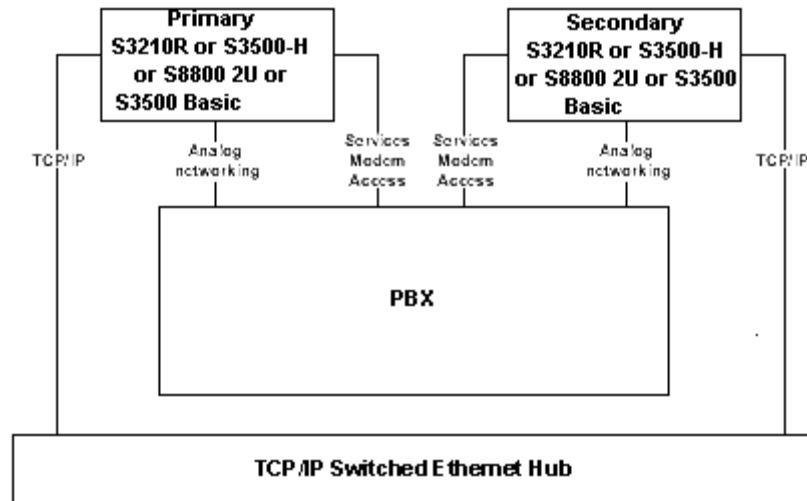
- RAID Level 5 disks (redundant and hot-swappable)
- Redundant and hot-swappable power supply
- Redundant and hot-swappable fans
- Required Uninterruptible Power Supply (UPS)

In the Attended High Availability Option scenario, a colocated, dedicated, spare server (referred to as the Secondary Message Networking application) is required for each live Message Networking application (known as the Primary Message Networking application). The server and software (Avaya Message Networking software) configuration of the Secondary Message Networking application must be exactly the same as that of the live Message Networking application for which it is backing up. The primary and secondary servers must be of the same type:

- If the primary Message Networking server is an S3210R, then the secondary must also be an S3210R.
- If the primary Message Networking server is an S3500-H, then the secondary must be an S3500-H respectively.
- If the primary Message Networking server is an S3500 Basic, then the secondary must be an S3500 Basic respectively.
- If the primary Message Networking server is an S8800 2U, then the secondary must be an S8800 2U respectively.

Note: If you do not want the secondary server to be colocated with the primary, then it must at least be on the same IP subnet as the primary. This is required so that the secondary can assume the same IP address as the primary system if it is down. In addition, if analog connectivity is required, then the switch providing that connectivity must be programmable such that it can forward those analog calls to the ports on the secondary system. These requirements are necessary to alleviate the re-administration of the remote message servers when accessing the primary or secondary systems.

The following figure provides a graphical depiction of the high-availability option.



There are two connectivity options for the Secondary Message Networking application:

Option 1: Connected Secondary Message Networking:

- LAN connectivity:
 - TCP/IP connected to the LAN.
 - IP Address of Secondary Message Networking configured to not conflict with Primary Message Networking during normal day-to-day operations.
- Switch connectivity:
 - Analog Networking Ports connected to the switch.
 - Services Modem connected to analog switch port (if alarms are not the problem).
 - Switch translations for all port types such that incoming calls do not occur until disaster recovery procedures are in place.

Option 2: Disconnected Secondary Message Networking:

- LAN Connectivity
 - TCP/IP not connected to the LAN
 - IP Address of Secondary Message Networking configured to be equal to the Primary Message Networking
- Switch Connectivity
 - Analog Networking Ports not connected to switch.
 - Services Modem not connected to analog switch port.

Note: It is possible to configure the Disconnected Secondary Message Networking (using A/B switches for example) so that it would be much faster to put into service and less error prone than the Connected Secondary Option.

Please note the following considerations regarding the attended high-availability option:

- The estimated down time is approximately 2 hours.
- Voice names are not restored unless an Attended Backup of the Primary Message Networking is executed.
- Messages/Status Messages/Remote Updates in queue on the Primary Message Networking when it goes down are lost.

There are [administration procedures](#) required to support the high-availability option daily, as well as procedures you must follow if you must put the secondary Message Networking into services.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Supported networking types



Supported networking types

This topic provides an introduction to the basics of Message Networking networking. Networking is the transfer of messages between users located on remote machines through Message Networking. Message Networking supports a number of [remote machine types](#). The following types of networking are supported:

- [Digital networking](#)
- [AMIS Analog Networking](#)
- [Octel Analog Networking](#)

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Message Networking networking > Digital networking

Digital networking

Digital networking is the transfer of a digital file from a subscriber on one system to a subscriber on another system. Voice and fax messages are files that are digitally recorded and stored. Digital networking allows these messages to be transferred from one remote machine to another using Message Networking.

A digital message is sent in the following manner:

1. A subscriber on a remote machine records a voice message or creates a fax or email message and then addresses it to a subscriber on a different remote machine.

Notes:

- Fax is supported on Aria and Serenade Digital, DEFINITY ONE Release 2.0, and systems using the VPIM V2 protocol. Email is supported on INTUITY AUDIX Release 4.0 or later, DEFINITY ONE Release 2.0, and systems using the VPIM V2 protocol. INTUITY digital networking and SMTP/MIME can pass text and binary files.
 - Digital networking on the Message Networking system uses an IP address since the digital protocol is TCP/IP.
2. Message Networking answers the call and identifies the remote machine and subscriber to whom the message is being sent.
 3. Message Networking sends the message, including a message header (remote machine name, sender's name, time the message was sent, and length of the message), to the remote subscriber.
 4. For AUDIX, the subscriber sending the message receives notification that the message was received.

TCP/IP is used to communicate with INTUITY AUDIX Release 4.0 or later, Aria Digital, Serenade Digital, VPIM V2, and SMTP/MIME digital systems, as well as between Message Networking systems.

TCP/IP networking has some impact on the amount of traffic over a system's LAN connection. You can calculate this impact by multiplying the number of networked messages by the number of packets and/or number of bytes per message.

TCP/IP networking LAN traffic example

For AUDIX, during the busy hour, a single remote system generates 150 voice messages, 30 fax messages, and 50 email messages using TCP/IP networking. The impact on the LAN can be calculated as follows:

KB:	$[(150 \times 135,000) + (150/2 \times 100) + (30 \times 144,000) + (30/2 \times 100)$ $+ (50 \times 5500) + (50/2 \times 100)] = 24.8 \text{ MB/hour}$
Packets:	$[(150 \times 135) + (30 \times 144) + (50 \times 5.5)] = 24,845 \text{ 1K data}$ packets/hour $[(150 \times 135)/2 + (30 \times 144)/2 + (50 \times 5.5)/2] = 12,423 \text{ 100 byte}$ ACK packets/hour
Total:	37,268 packets/hour

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

Getting Started

Administration

Installation

Maintenance

Reference

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Message Networking networking > AMIS Analog Networking



AMIS Analog Networking

AMIS Analog Networking plays messages as voice files over analog lines to communicate with other AMIS Analog systems (Avaya and non-Avaya AMIS systems).

An AMIS Analog message is sent in the following manner:

1. A subscriber on a remote machine records a voice message and addresses the message to an AMIS subscriber on another remote machine.
2. The AMIS Analog protocol sends the message to the Message Networking system.
3. Message Networking answers the call and identifies the remote machine and subscriber to whom the message is being sent.
4. Message Networking sends the message to the remote subscriber using the AMIS Analog protocol.
5. The remote AMIS Analog machine answers the call, exchanges protocols with the Message Networking system, and allows Message Networking to play, *not* transfer, the message.
6. The remote AMIS Analog machine records the message, as it is played, into the mailbox of the subscriber receiving the message.
7. The receiver can now listen to the message.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

Getting Started

Administration

Installation

Maintenance

Reference

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Message Networking networking > Octel Analog Networking



Octel Analog Networking

Octel Analog Networking sends messages as voice or fax files over analog lines to communicate with other analog systems (Avaya and non-Avaya analog systems).

Note: Octel Analog Networking can also be used to network with Unified Messenger and Octel 100 systems for voice messages only.

A message is sent in the following manner:

1. A subscriber on a remote machine records a voice message and addresses the message to a subscriber on a different remote machine.
2. The Octel Analog Networking protocol sends the message to the Message Networking system.
3. Message Networking answers the call and identifies the remote machine and subscriber to whom the message is being sent.
4. Message Networking sends the message to the remote subscriber using Octel Analog Networking protocol.
5. The remote machine answers the call, exchanges protocols with the Message Networking system, and allows Message Networking to play, *not* transfer, the message.
6. The remote machine records the message, as it is played, into the mailbox of the subscriber receiving the message.
7. The receiver can now listen to the message.

[Top of page](#)





Supported remote machine types

Message Networking supports the following remote machines:

- **AUDIX Digital (TCP/IP):**
 - INTUITY AUDIX
 - INTUITY AUDIX LX
 - DEFINITY ONE Release 2.0
 - IP600 Release 9.2.1 and later
 - Avaya IA770
- **AMIS Analog:**
 - DEFINITY AUDIX
 - Other vendors that support AMIS Analog
- **Octel Analog:**
 - Aria Release 2.X and later (250SX, 250, and 350 models)
 - Serenade Release S.2.0.X and later (200SX, 200, and 300 models)
 - Octel 100 Release 3.2.9d and later
 - Unified Messenger Release 3.0 and later (UM for Microsoft Exchange)
 - Avaya Modular Messaging with Microsoft Exchange (for Modular Messaging releases that support Microsoft Exchange)
Note: Octel Analog Networking is not supported for Modular Messaging/Exchange systems using H.323 integrations.
 - Alcatel 4635 4.02 and later
- **Aria Digital:**
 - Release 2.05 and later and A3.X (250SX, 250, and 350 models)
Note: Aria 3.0 is not supported; it must be upgraded to 3.01.
 - Alcatel 4635 4.02
- **Serenade Digital Release S2.0 and later** (200SX, 200, and 300 models)
- **VPIM V2 Digital networking**
- **LDAP Client:**
 - A remote machine administered as an LDAP Client can be used to perform queries of Message Networking system data and to perform system administration
- **SMTP/MIME:**
 - Modular Messaging/MSS Release 2.0 and later systems (includes LDAP-based directory updates)
Note: Modular Messaging/MSS Release 1.1 and earlier systems are not supported. These systems must be upgraded to Modular Messaging/MSS Release 2.0.
 - Modular Messaging MultiSite Release 5.0 and later systems (includes LDAP-based directory updates)
 - Avaya Aura™ Messaging (includes LDAP-based directory updates)

- Message Networking Release 2.0 and later systems (includes LDAP-based directory updates)
Note: Message Networking Release 1.1 and earlier systems are not supported. These systems must be upgraded to Message Networking Release 2.0.
- Other vendors (email) with GSM or G.711(mu and A-law) voice encoding

See the [Remote machine overview](#) for more information on the remote machine types that Message Networking supports.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Remote machine overview



Remote machine overview

Remote machines are end points with which Message Networking can communicate through network protocols.

This topic provides the following information on the [remote machines](#) and networking protocols supported by Message Networking:

- [Digital protocol information](#)
- [Supported component types](#) by machine type
- [Feature support](#) by protocol type
- [Maximum number of recipients per message](#) by machine type
- [Subscriber directory updates to remote machines](#)
- [Message Confirmation support comparison](#)
- [Average number of subscribers](#) by connection type
- [Remote machine considerations](#)

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machine overview](#) > Comparison of digital protocol information



Comparison of digital protocol information

The following table compares the digital protocols supported for use by Message Networking.

TCP/IP protocol	Encoding algorithm	Bytes/second	Average voice message (60 seconds) including overhead	Average fax message (3 pages) including overhead	Average subscriber update length (from/to, assuming a 3-second voice name)	TCP/IP port used
AUDIX Digital	Code-Excited Linear Programming (CELP)	2K	135K bytes	230K bytes	6K bytes	5500 (decimal)
Aria Digital	Sub-band Coding (SBC)	3K	250K bytes	450K bytes	9K bytes	4000 (decimal)
Serenade Digital	Continuously Variable Sloped Delta Modulation (CVSD)	3K	250K bytes	450K bytes	9K bytes	22136 (decimal)
SMTP/MIME	Global Specification for Mobile Communication (GSM)	1.7K	140K bytes	350K bytes	LDAP-based: 24K bytes	25 and 465 (decimal)
	G.711 μ -law and A-law	8K	660K bytes			25 and 465 for messages (55389 for Avaya MM LDAP, 56389 for Message Networking LDAP, 55389 for Avaya Aura™ Messaging LDAP)
VPIM	Adaptive Digital Pulse Code Modulation (ADPCM)	4K	330K bytes	350K bytes	12K bytes	25 (decimal)

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#) [Administration](#) [Installation](#) [Maintenance](#) [Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machine overview](#) > Message Networking message component types

Message Networking message component types

The following table lists the maximum number of recipients of inbound and outbound messages for each supported protocol:

Product	Protocol	Voice	Fax	Text	Binary	Annotation/ subject
Other vendor	AMIS	Y	N	N	N	N
Modular Messaging/MSS	SMTP/MIME	Y	Y	Y	Y	Y
Modular Messaging MultiSite/MSS	SMTP/MIME	Y	Y	Y	Y	Y
Modular Messaging/Exchange	Octel Analog Networking	Y	Y (see note)	N	N	N
INTUITY AUDIX Release 3	AUDIX Digital TCP/IP	Y	Y	N	Y	Y
INTUITY AUDIX Release 4 and 5	AUDIX Digital TCP/IP	Y	Y	Y	Y	Y
INTUITY AUDIX LX Release 1.0 and greater	AUDIX Digital TCP/IP	Y	Y	Y	Y	Y
DEFINITY ONE Release 2.0, IP600, IA770	AUDIX Digital TCP/IP	Y	Y	Y	Y	Y
DEFINITY AUDIX	AMIS	Y	N	N	N	N
Aria Release 1.0 and greater	Octel Analog Networking	Y	Y	N	N	N
Aria Release 2.05 and greater	Aria Digital TCP/IP	Y	Y	N	N	N
Serenade Release S2.0 and greater	Octel Analog Networking	Y	Y	N	N	N
Serenade Release S2.0 and greater	Serenade Digital TCP/IP	Y	Y	N	N	N
Unified Messenger Release 3.0 and greater (Microsoft Exchange)	Octel Analog Networking	Y	Y (see note)	N	N	N
Octel 100 Release 3.2.9d	Octel Analog Networking	Y	N	N	N	N
VPIM systems	VPIM TCP/IP	Y	Y	Y (see note)	N	Y
SMTP/MIME systems	SMTP/MIME TCP/IP	Y	Y	Y	Y	Y

Notes:

- Support for the text component type is vendor-dependent.
- Modular Messaging/Exchange system require a separate fax server to support fax components.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Index](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Feature support by protocol type

Feature support by protocol type

The following tables outline the Message Networking support of features by protocol type.

Message Networking feature	INTUITY AUDIX	Octel Analog and Aria Digital	Serenade Digital
Analog Encryption	Not supported	Supported for Octel Analog	Not supported
Annotation	Supported Release 4.0.0 or later	Not supported	Not supported
Automatic Message Forwarding	Not supported	Supported	Supported
Update of Remote Subscriber Records on remote machines	Supported	For Octel Analog, add and change supported; delete not supported For UM: not supported For Aria Digital, add/change/delete/message delivery supported	Add/change/ message delivery supported; delete not supported
Update of Subscriber Records on the Message Networking system	Supported	For Octel Analog, add and change supported; delete not supported UM: if "default" record exists on the Message Networking system. Subscribers are updated on Message Networking from the Unified Messenger directory only if a default record for the subscriber exists in the Message Networking directory. For Aria Digital, add/change/delete/message delivery supported	Add and change supported; delete not supported (in general, oriented toward sender validation)
Binary	Supported for Release 4.0.0 or later	Not supported	Not supported
Bulk Subscriber Additions/ Changes/	Not supported; not required for digital	Supported; not required for digital	Not required

Deletions by File Ranges			
Call Detail Recording (CDR)	Supported	Supported	Supported
Component Delivery	Sends the components that Message Networking can deliver, along with a voice message to the recipient to indicate that one or more components were undeliverable	Sends the components that Message Networking can deliver, along with a voice message to the recipient to indicate that one or more components were undeliverable	Sends the components that Message Networking can deliver, along with a voice message to the recipient to indicate that one or more components were undeliverable
Data/ Message Encryption	Not supported	Supported for Aria Digital	Not supported
Demand Remote Updates	Supported	Supported by range; preferred method is with NameSend from Aria node	Performed by executing push from end node called NameSend
Dial by ASCII Name	Supported	Supported	Supported
Dial Plan Mapping	Supported	Supported	Supported
Directory Views (dynamic, with voiced name option)	Supported	Supported	Supported
Directory Views (static, with voiced name option)	Supported (with remote machine pull from INTUITY AUDIX at initialization)	Supported with Message Networking; remote machine push at initialization for Aria Digital	Supported with Message Networking; remote machine push at initialization
Failed Message Delivery from Message Networking	Supported with two incoming messages: <ul style="list-style-type: none"> Failed message notification Original copy of message 	Supported with two incoming messages: <ul style="list-style-type: none"> Failed message notification Original copy of message 	Supported with two incoming messages: <ul style="list-style-type: none"> Failed message notification Original copy of message
Failed Message Delivery to Message Networking	Supported	Supported	Supported
Fax	Supported for release 3.0 or later	Supported for Release 2.03 or later for Aria Digital. Not supported for Unified Messenger and Octel 100.	Supported for Release 2.0 or later

Forwarding a Message	Supported	Supported	Supported; Serenade to Serenade or Aria "forwarded" messages have this indicated in message header
Forward and Reply Indication to Recipient	Supported when subscriber replying or forwarding is a Serenade Octel Analog subscriber	Supported when subscriber replying or forwarding is a Serenade Octel Analog subscriber	Supported for Serenade Digital to Serenade Digital
Future Delivery	Supported	Supported from Aria Digital to Aria Digital and Octel Analog only. Not supported for the following: Aria, UM, and Octel 100 to AUDIX, AMIS, Serenade Digital, and VPIM V2	Supported
Inbound Analog Fallback	Not supported	Not supported	Not supported
Maximum Number of Recipients per Single Message Transmission (inbound)	250	Octel 250/350 Analog: 100 X bad connection count in System Parameter Networking screen UM: unlimited Aria Digital: unlimited Octel 200/300 Analog: 10	10
Maximum Number of Recipients per Single Message Transmission (outbound)	250	Octel 250/350 Analog: 250 but tunable to fewer UM: 250 Octel 200/300 Analog: 250 but tunable to fewer (still stores in groups of 10) Aria Digital: 250 (not tunable)	10
Message Delivery Confirmation	Supported	Supported	Supported
Multi-language Message Responses from Message Networking Network	Installed languages	Installed languages	Installed languages
Multiple Simultaneous Connections from the Same Remote Machine	Not supported	Supported for Octel Analog; not supported for Aria Digital	Not supported

(Inbound)			
Multiple Simultaneous Connections from the Same Remote Machine (Outbound)	Not supported	Supported for Octel Analog Not supported for Aria Digital	Not supported
Name Confirmation (spoken)	Supported	Supported	Supported
Network Turnaround	Supported	Not supported	Not supported
Outbound Analog Fallback	Not supported	Not supported	Not supported
Overlapping Prefixes/ Multiple Prefixes per Location	Supported	Supported	Supported
Priority Message Indication	Supported	Supported	Supported
Private or Urgent Message Indication	Supported	Supported (user hears "priority" notice vs. urgent)	Supported (user hears "priority" notice vs. urgent)
Receiving a Voice Message	Supported	Supported	Supported
Receiving Voiced Name of Sender	Sender's name in message header	Sender's name in message header	Sender's name in message header
Recipient Name Confirmation when Addressing a Message	Supported	Supported	Supported
Remote Machine Reports	Supported	Supported	Supported
Reply to a Network Message	Supported	Supported	Supported; replied to messages have this indicated in message header
Accessed Return-Receipt/ Confirmation	See Message confirmation support	See Message confirmation support	See Message confirmation support
Self-Registration Agent	Not supported for digital	Not supported for digital	Not supported for digital

Sending a Message to an Aria Recipient with Extended Absence Greeting (EAG) block activated	Sender receives a failed message	Sender receives a failed message	Sender receives a failed message
Sending a Message to an Aria Recipient with Extended Absence Greeting (EAG) warning activated	Sender receives an EAG warning message	Sender receives an EAG warning message	Sender receives an EAG warning message
Sending a Voice Message	Supported	Supported	Supported
Subscriber Community ID	Supported (default is 1)	Supported (default is 1)	Supported (default is 1)
Subscriber NetName Type	Supported (default is u)	Supported	Supported (default is u)
Subscriber Reports	Supported	Supported	Supported
Text Message	Supported for Release 4.0.0 or later	Not supported	Not supported
Time of Day Routing	Supported	Not supported for outbound	Not supported for outbound
Traffic Reports			
Network Load	Supported	Supported	Supported
Network Status	Supported	Supported	Supported
Port Utilization	Supported with selection by protocol resource type	Supported with selection by protocol resource type	Supported with selection by protocol resource type
Weekend/Holiday/Message Type Routing from Message Networking	Not supported	Not supported	Not supported

Message Networking feature	AMIS Analog	VPIM V2	SMTP/MIME
Analog Encryption	Not supported	N/A	N/A

Annotation	Not supported	Supported as determined by the remote machine	Yes
Automatic Message Forwarding	Supported as determined by the remote machine	Supported as determined by the remote machine	Supported as determined by the remote machine
Update of Remote Subscriber Records on remote machines	Not supported	Not supported	Supported for Avaya Modular Messaging with LDAP
Update of Subscriber Records on the Message Networking system	Not supported	Not supported	Supported for Avaya Modular Messaging with LDAP
Binary	Not supported	Not supported	Yes
Bulk Subscriber Additions/ Changes/ Deletions by File Ranges	Supported	Supported	Supported (except for Avaya Modular Messaging which does not require this feature)
Call Detail Recording (CDR)	Supported	Supported	Supported
Component Delivery	Sends the components that Message Networking can deliver, along with a voice message to the recipient to indicate that one or more components were undeliverable	Sends the components that Message Networking can deliver, along with a voice message to the recipient to indicate that one or more components were undeliverable	Sends all
Data/ Message Encryption	Not supported	Not supported	Not supported
Demand Remote Updates	N/A	Not supported	Supported for Avaya Modular Messaging with LDAP
Dial by ASCII Name	Supported as determined by the remote machine	Supported as determined by the remote machine	Supported as determined by the remote machine
Dial Plan Mapping	Supported	Supported	Supported
Directory Views (dynamic, with voiced name option)	N/A	Dynamic only	Dynamic for non-LDAP

Directory Views (static, with voiced name option)	N/A	Not supported	Not supported
Failed Message Delivery from Message Networking	Supported with two incoming messages: <ul style="list-style-type: none"> Failed message notification Original copy of message 	Supported with Nondelivery Notification (NDN) and single incoming message (DSN) containing: <ul style="list-style-type: none"> Failed message notification Original copy of message 	Supported with Nondelivery Notification (NDN) and single incoming message (DSN) containing: <ul style="list-style-type: none"> Failed message notification Original copy of message
Failed Message Delivery to Message Networking	Supported	Supported	Supported
Fax	Not supported	Supported as determined by the remote machine	Supported as determined by the remote machine
Forwarding a Message	Supported as determined by the remote machine	Supported as determined by the remote machine	Supported as determined by the remote machine
Forward and Reply Indication to Recipient	Supported when subscriber replying or forwarding is a Serenade Octel Analog subscriber	Not supported	Not supported
Future Delivery	Supported as determined by the remote machine	Supported as determined by the remote machine	Supported as determined by the remote machine
Inbound Analog Fallback	N/A	Not supported	Not supported
Maximum Number of Recipients per Single Message Transmission (inbound)	1	1000	1000
Maximum Number of Recipients per Single Message Transmission (outbound)	1	250	250
Message Delivery Confirmation	Not supported	Supported as delivery to Message Networking	Supported as delivery to Message Networking
Multi-	Installed languages	Installed languages	Installed languages

language Message Responses from Message Networking Network			
Multiple Simultaneous Connections from the Same Remote Machine (Inbound)	Supported as determined by remote machine	Not supported	Not supported
Multiple Simultaneous Connections from the Same Remote Machine (Outbound)	Supported for up to 9 sessions	Not supported	Not supported
Name Confirmation (spoken)	Supported as determined by the remote machine	Supported as determined by the remote machine	Supported as determined by the remote machine
Network Turnaround	N/A	Not supported	Not supported
Outbound Analog Fallback	N/A	Not supported	Not supported
Overlapping Prefixes/ Multiple Prefixes per Location	Supported as determined by the remote machine	Supported as determined by the remote machine	Supported as determined by the remote machine
Priority Message Indication	Supported, except for priority message originating from an AMIS sender	Supported	Supported
Private or Urgent Message Indication	Supported, except for private message originating from an AMIS sender	Supported as determined by the remote machine	Supported as determined by the remote machine
Receiving a Voice Message	Supported	Supported	Supported
Receiving Voiced Name of Sender	Sender's name in message header	Sender's name in message header	Supported for Avaya Modular Messaging
Recipient Name Confirmation when Addressing a Message	Supported as determined by the remote machine	Supported as determined by the remote machine	Supported as determined by the remote machine
Remote Machine Reports	Supported	Supported	Supported
Reply to a Network	Supported as determined by the	Supported as determined by the	Supported as determined by the

Message	remote machine	remote machine	remote machine
Accessed Return-Receipt/Confirmation	N/A	See Message confirmation support	See Message confirmation support
Self-Registration Agent	Supported	Supported	Supported for non-LDAP; not supported for Avaya Modular Messaging (LDAP)
Sending a Message to an Aria Recipient with Extended Absence Greeting (EAG) block activated	Sender receives a failed message	Sender receives a failed message	Sender receives a failed message
Sending a Message to an Aria Recipient with Extended Absence Greeting (EAG) warning activated	Sender receives an EAG warning message	Sender receives an EAG warning message	Sender receives an EAG warning message
Sending a Voice Message	Supported	Supported as determined by remote machine	Supported
Subscriber Community ID	Supported (default is 1)	Supported (default is 1)	Supported (default is 1)
Subscriber NetName Type	Supported (default is u)	Supported (default is u)	Supported (default is u)
Subscriber Reports	Supported	Supported	Supported
Text Message	Not supported	Supported	Supported
Time of Day Routing	Not supported	Not supported for outbound	Not supported for outbound
Traffic Reports			
Network Load	Supported	Supported	Supported
Network Status	Supported	Supported	Supported
Port Utilization	Supported with selection by protocol resource type	Supported with selection by protocol resource type	Supported with selection by protocol resource type
Weekend/Holiday/Message Type Routing from Message Networking	Not supported	Not supported	Not supported

Future delivery considerations

Remote machines in a Message Networking network handle future delivery messages in one of two ways:

- The sending machine stores the future-dated message and then sends the message to its receiving machine at the stipulated time. The receiving machine then immediately distributes the message to the recipient. Unified Messenger using Octel Analog Networking, Serenade, and INTUITY AUDIX Digital (DEFINITY ONE Release 2.0, INTUITY AUDIX Release 4.0 or later, IP600 Release 9.2.1, Avaya IA770, and INTUITY AUDIX LX Release 1.0 and greater) remote machines store messages marked for future delivery until the stipulated time.
- The sending machine does not store the future-dated message, but instead sends it immediately to the receiving machine. The receiving machine then stores the message and distributes it to the recipient at the stipulated time. Aria, and Octel 100 remote machines do not hold future delivery messages and instead send them immediately. These types of remote machines expect the receiving system to display the message at the appropriate time.

Note: All messages received from VPIM V2 and SMTP/MIME systems are assumed to be delivered as soon as normal delivery schedules permit. VPIM and SMTP/MIME machines can receive future delivery messages if they are sent by a machine that holds future delivery messages and then sends them at the time specified.

In either case, Message Networking does not control the sending and receiving of future delivery messages. Message Networking rejects future delivery messages that are scheduled to be delivered before the expected date. Most sending end nodes hold a future delivery message until it is time to send it. In these cases, Message Networking ignores the future delivery flag and sends the message.

In cases where the sending machine does not hold the message, Message Networking verifies that the receiving machine will hold the message. If the receiving machine will not hold the message, Message Networking rejects the message.

In a configuration where there are multiple Message Networking systems and the sender is on one hub and the recipient on another, the sent message is delivered immediately.

Failed delivery notification considerations

Note the following considerations related to failed message notification:

- When the same message fails to be sent to multiple recipients, Message Networking groups all of the failed recipients into one failure notification message.
- Extended Absence Greeting blocks are treated as a failed message delivery by Message Networking.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

Getting Started

Administration

Installation

Maintenance

Reference

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machine overview](#) > Maximum number of recipients per message

Maximum number of recipients per message

The following table lists the maximum number of recipients of inbound and outbound messages for each supported protocol.

Protocol	Inbound	Outbound
AMIS	1	1
AUDIX Digital	250	250
DEFINITY AUDIX	40 (250 in DEFINITY AUDIX 3.2-7 and 4.0)	40 (250 in DEFINITY AUDIX 3.2-7 and 4.0)
Aria/Unified Messenger using Octel Analog Networking	100 times bad connection count in System Parameter Networking screen (max 10000)	250, but tunable to fewer
Octel 100	99 times number of attempts count under Node Profile (max 9900)	250, but tunable to fewer
Serenade Octel Analog Networking	10	10
Aria Digital	Unlimited	250, but tunable to fewer
Serenade Digital	10	10
SMTP/MIME	1,000	250
VPIM	1,000	250

[Top of page](#)





[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machine overview](#) > Subscriber directory updates to remote machines



Subscriber directory updates to remote machines

This topic provides an overview of subscriber directory updates to Message Networking remote machines.

The directory update type determines the Message Networking subscribers that are populated to a new remote machine and included in updates to a remote machine. You specify the type of directory updates in the **Subscriber Updates Type** field on the **Remote Machine Parameters** page for a specific remote machine.

Note: How subscribers are populated to new remote machines and how updates are initiated to remote machines depends on the remote machine type. See the [Adding and updating subscribers overview](#) for additional information about how subscribers are added and updated on Message Networking remote machines.

Message Networking supports the following types of directory updates:

Full updates. Full updates include every subscriber on every system in the Message Networking network. This option ensures that subscribers on the new system can address by name every subscriber in the network. However, this option can require a large amount of disk space on the new system. Also, remote subscribers who do not send or receive messages will be stored unnecessarily. To specify full updates for a remote machine, select **full** as the **Subscriber Updates Type** on the **Remote Machine Parameters** page.

If you select full updates, Message Networking performs a full update when you first administer the new system and run a Demand Remote Push to the new system. Subsequent updates occur in either of the following circumstances:

- When you perform a Demand Remote Push for the remote machine.
- When Message Networking receives a subscriber change from a remote machine.

Caution! If you begin with full updates or later change to dynamic updates, Message Networking removes all subscribers from the remote subscriber directory and begins to repopulate the directory with dynamic updates.

Dynamic updates. With this update option, each time a subscriber on the new system sends a message to a remote subscriber, that remote subscriber is added to the Dynamic Directory List for the new system. Likewise, each time a remote subscriber sends a message to a subscriber on the new system, that remote subscriber is added to the list. To specify dynamic updates for a remote machine, select **dynamic** as the **Subscriber Updates Type** on the **Remote Machine Parameters** page.

If, typically within the next 90 days (as set on the **Dynamic Sub Expiration Days** on the **General Parameters** page), no other messages are sent from the new system to that remote subscriber or vice versa, that remote subscriber is removed from the list. This removal helps save storage space on the new system.

Directory View updates only. With this option, the new system's remote subscriber list includes subscribers within ranges of extensions on the systems you specify. A Directory View list for a system is static and, as with full updates, this option can use a lot of disk space. Additionally, with this option, subscribers who fall outside of the ranges and systems you specify are not addressable by name from the new system. To specify directory view updates for a remote machine, select **directory-view** as the **Subscriber Updates Type** on the **Remote Machine Parameters** page.

If you select directory view updates, Message Networking performs a Directory View update when you first administer the new system and run a Demand Remote Push to the new system. Subsequent updates include changes to subscriber lists of remote systems, where subscribers are added or removed. Subsequent updates occur in either of the following ways:

- When you perform a Demand Remote Push for this system
- When Message Networking receives a subscriber change from a remote system.

Combination of dynamic and Directory View updates. You can use dynamic and Directory View updates in

combination. In this case, dynamic updates occur as described above, but the Directory Views option also identifies specific ranges of extensions on specific remote machines to ensure that remote subscribers on those systems can be addressed by name on the new system. To specify this combination for a remote machine, select **directory-view** as the **Subscriber Updates Type** on the **Remote Machine Parameters** page and then [add a directory a view](#) for the remote machine.

This type of setup is useful when you are converting a high-traffic point-to-point system to the Message Networking network or when it is important that all or a subset of remote subscribers on a specific system are addressable by name for subscribers on the new system.

The following table provides a comparison of the network directory update types supported for each type of remote machine. The directory update types listed are the Subscriber Update

Protocol Type	Full	Directory View	Dynamic	None
AMIS	No	No	No	No
AUDIX Digital (including DEFINITY ONE and IP600)	Yes	Yes	Yes	Yes
Octel Analog Networking	Yes	Yes	Yes	Yes
Aria Digital	Yes	Yes	Yes	Yes
Serenade Digital	Yes	Yes	Yes	Yes
VPIM	No	No	Yes	No
SMTP/MIME	Required for MM and Avaya Aura™ Messaging systems with an Avaya message Store and remote MN systems	Yes (for MM/Avaya Message Store/ Avaya Aura™ Messaging)	SMTP/MIME systems other than MM/Avaya Message Store, Avaya Aura™ Messaging and MN systems	Yes (for MM/Avaya Message Store and Avaya Aura™ Messaging)

Note: Modular Messaging and Avaya Aura™ Messaging systems do not accept more than 250,000 subscribers (with or without voice names) during an update. Therefore, if the Message Networking system has more than 250,000 subscribers and you are updating to a Modular Messaging and Avaya Aura™ Messaging remote machines, you must [administer the Modular Messaging and Avaya Aura™ Messaging remote machines](#) to use directory view updates. The [directory view](#) you administer for the Modular Messaging and Avaya Aura™ Messaging systems must include not more than 250,000 subscribers.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machine overview](#) > Message confirmation support

Message confirmation support

The following table compares accessed/return receipt/positive confirmation and negative confirmation support for messages sent through the Message Networking.

Accessed/return receipt/positive confirmation support

The following table lists whether senders who request message notification are notified when their message has been played.

Note: Information in the AUDIX rows and columns also applies to DEFINITY ONE and IP600 systems.

Sender:	Receiver:									
	AUDIX	Aria Octel	Serenade Octel	AMIS Analog	Octel 100	UM	Aria Digital	Serenade Digital	VPIM	SMTP/MIME
AUDIX	Y	N	N	N	N	N	N	N	N	N
Aria Octel Analog	N	Y	Y	N	Y	Y	Y	N	N	N
Serenade Octel Analog	N	Y	Y	N	Y	Y	Y	N	N	N
AMIS Analog	N/A	N/A	N/A	N	N/A	N/A	N/A	N/A	N	N
Octel 100	N	Y	Y	N	Y	Y	Y	N	N	N
UM Exchange using Octel Analog	N	Y	Y	N	Y	Y	Y	N	N	N
Aria Digital	N	Y	Y	N	Y	Y	Y	N	N	N
Serenade Digital	N	N	N	N	N	N	N	Y	N	N
VPIM v2 Digital	N	N	N	N	N	N	N	N	Y (see note)	N
SMTP/MIME (including Avaya Modular Messaging and Avaya Aura™ Messaging)	N	N	N	N	N	N	N	N	N	N

Negative confirmation support

Negative confirmation support is a feature whereby senders who request message notification are notified when

a received message has not been played after a certain length of time. Message Networking only supports this feature when the recipient is on an Serenade Octel Analog or Aria Digital system.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Remote machine considerations



Remote machine considerations

This topic provides information on considerations for the remote machine types supported by Message Networking:

- [INTUITY AUDIX](#) (including DEFINITY ONE and IP600)
- [AMIS Analog](#)
- [Octel Analog Networking](#)
- [Unified Messenger](#) using Octel Analog Networking
- [Aria Digital and Serenade Digital](#)
- [VPIM](#)
- [SMTP](#):
 - [General considerations](#)
 - [Modular Messaging considerations](#)
 - [Avaya Aura™ Messaging](#)

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machines overview](#) > [Remote machine considerations](#) > INTUITY AUDIX remote machine considerations

INTUITY AUDIX remote machine considerations

The following are considerations related to INTUITY AUDIX remote machines:

- *Scheduled message* status for INTUITY AUDIX indicates that delivery has not been successfully completed, nor has it failed yet.
- Failed messages can exist in both incoming and outgoing mailboxes for INTUITY AUDIX.
- *Accessed* status is consistent on both the Message Networking and INTUITY AUDIX systems.
- Large messages to INTUITY AUDIX from Aria and Serenade are failed with a *message length* failure code. INTUITY AUDIX LX systems support a larger message length size than do INTUITY AUDIX Release 4 or 5 systems.
- When recipients of messages from INTUITY AUDIX, DEFINITY ONE, and IP600 systems are notified that one or more components of a multimedia message cannot be delivered, the sender is not notified. The recipient is notified to contact the sender for missing components.
- DEFINITY ONE and IP600 work in the same manner as does INTUITY AUDIX; therefore, DEFINITY ONE and IP600 systems do not support receipt of future delivery messages sent from Aria systems.
- When you want to send a message to all subscribers in an Enterprise using a single Enterprise List, the following suggestions can help to reduce network traffic load and the effects of MWIs:
 - Reference a single mailbox per server in an Enterprise List that has broadcast permission. Using this method, only one message is sent to each server. After the message is deposited in the subscriber's mailbox (with broadcast permission), the subscriber can then forward the message to the rest of the subscribers on the server with or without MWI.
 - Enterprise Lists can be created that reference local INTUITY AUDIX ELA lists containing all local subscribers. This method also cuts down on network traffic load. When using Enterprise Lists and INTUITY AUDIX ELA, make sure that a range defined on an Enterprise List does not include an ELA list (unless that is the desired effect). Additionally, be careful not to create a cycle by referencing an ELA list in an Enterprise List that references the same Enterprise List.
- There is an issue that can occur when you have a distribution list on an INTUITY AUDIX system (a personal list or an ELA list) that references remote Message Networking network addresses, and the Directory View for that INTUITY AUDIX system is quite large (usually greater than 10,000 remote subscribers). In this scenario, it is possible for the referenced network addresses to be deleted from the local INTUITY AUDIX list when a directory synchronization problem occurs during a Demand Remote Update between the two systems. When the Directory View is quite large and takes longer for a full update, the chance of the directory synchronization being interrupted and having to restart is greater (for example, because an audit has started). In some cases, this restart causes the remote subscribers on the INTUITY AUDIX system (the Message Networking network addresses) to be reassigned a new internal subscriber identifier (an internal number, not a new external network address). It is this internal subscriber identifier that is stored when the local INTUITY AUDIX list is built and, as a result, impacts the list. If this problem occurs, it is recommended that you create Enterprise Lists on the Message Networking system for these network addresses.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machines overview](#) > [Remote machine considerations](#) > AMIS Analog remote machine considerations

AMIS Analog remote machine considerations

The following are considerations related to AMIS Analog remote machines:

- AMIS messages are marked as Delivered upon successful delivery to the Message Networking system. AMIS protocol does not support Accessed status.
- Digital network mailboxes sending messages to AMIS subscribers that are administered on the Message Networking system can address messages using the subscribers' numbers or names.
- Optional voiced names are supported for AMIS subscribers.
- Messages received by digital network mailboxes from AMIS subscribers are treated as though they are coming from another digital network mailbox. The recipient hears "Message from *voice or extension*."
- AMIS subscriber messages can optionally contain the Private/Priority designation and voiced name of the sender as part of the actual message being sent.
- When recipients of messages from AMIS Analog systems are notified that one or more components of a multimedia message cannot be delivered, the sender is not notified. The recipient is notified to contact the sender for missing components.
- Optional voiced names are supported in messages sent from INTUITY AUDIX, Octel Analog Networking, Aria Digital, Serenade Digital, and VPIM subscribers to AMIS mailboxes.
Note: Optional voiced names in messages sent from VPIM V2 senders are supported if the VPIM remote machine can send voiced names.
- Optional Private/Priority designations are supported in messages sent from INTUITY AUDIX, Octel Analog Networking, Aria Digital, Serenade Digital, VPIM, and SMTP/MIME subscribers to AMIS subscribers.
- Sending messages to large Enterprise Lists using AMIS Analog is not recommended as AMIS Analog delivers a message once for each recipient receiving a message.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machines overview](#) > [Remote machine considerations](#) > Octel Analog Networking remote machine considerations

Octel Analog Networking remote machine considerations

This topic provides considerations related to Octel Analog Networking remote machines.

Note: For specific considerations related to Modular Messaging/Exchange systems that use Octel Analog Networking, see [Modular Messaging remote machine considerations](#) and [Avaya Aura™ Messaging remote machine considerations](#)

General considerations

The following general considerations are related to Octel Analog Networking remote machines:

- Reply to sender of analog messages is supported.
- Playback of name during message addressing and directory searches for registered subscribers (for those sending from AUDIX, Aria, or Serenade, not AMIS) are supported.
- Automatic directory updates are supported.
Note: Subscribers are updated on the Message Networking system from the Unified Messenger directory only if a default record for the subscriber exists in the Message Networking directory. For more information about creating default records, contact the Professional Services Organization (PSO).
- Voice name in messages sent from INTUITY AUDIX, Aria Digital, and Serenade Digital subscribers to Octel Analog Networking subscribers are supported.
- Message designations sent from INTUITY AUDIX, Aria Digital, and Serenade Digital subscribers to Octel Analog Networking subscribers are changed from Priority and Private to Urgent and Private.
- Undeliverable messages are automatically returned to sender on other remote machines.
- The Message Networking system allows a network address of 3 to 10 digits. A 10-digit dial plan is recommended.
- A subscriber on a remote system must be registered on a Message Networking system for that Message Networking system to accept messages for delivery.
- A *scheduled message* status indicates that delivery has not been successfully completed, nor has it failed yet.
- Senders receive notification of failed messages in two ways, including:
 - An error message indicating each mailbox that failed to receive the sent message. This can be an optional Priority message.
 - A copy of the failed original message from the Failed Message Delivery Manager.
- When sending a fax message to a recipient on an Octel Analog Networking node or an Aria Digital node, the sender must include a voice message. If the fax is sent without a voice message, the Message Networking system adds a default voice component to the message.
- Unified Messenger and Octel 100 can exchange voice, but not fax, messages. If a Unified Messenger or Octel 100 user receives a voice message with a fax attached, the fax is discarded, and the user is asked to contact the sender.
- Large messages (approximately 20 minutes in length) sent to an INTUITY AUDIX remote machine from an Octel Analog Networking remote machine through the Message Networking system are failed with a *message length* failure code.
- When an Octel Analog Networking Aria sender sends a mixed Private and Priority message to multiple

INTUITY AUDIX recipients and has marked any of the recipients as Priority or Private on the same remote machine, the message is marked as Priority or Private to all recipients.

- The forward and reply indicators for recipients are supported when the sender of a message through the Message Networking system is an Octel Analog Networking Serenade subscriber.
- For Demand Remote Push:
 - When executing the Demand Remote Push, be aware that it takes 25 seconds per subscriber to update the remote Octel Analog Networking machine. Thus, if you have 1,000 subscribers to be updated on the remote machine, this function takes approximately eight hours to run.
 - Demand Remote Push updates are not supported for Octel 100 remote machines.
- If three messages are already in the queue for a port and the maximum number of simultaneous ports for an Octel Analog Networking remote machine has not been exceeded, then the system starts a new port.
- Network turnaround is not supported for Octel Analog Networking remote machines.
- Multiple simultaneous sessions (inbound and outbound) to an Octel Analog Networking remote machine are supported.
- Encryption of DTMF is supported.
- Different term definitions used by the Message Networking and Octel Analog Networking machines:
 - *Notice* indicates a positive message confirmation for an Octel Analog Networking remote subscriber.
 - *Message* indicates a message failure from the Message Networking system.
- If the remote machine is Unified Messenger, an Octel gateway must be administered on the Unified Messenger system for messages to be transmitted properly. For more information about the steps required to administer the Octel gateway, see the Unified Messenger documentation.

Octel 100 Octel Analog considerations

The following considerations are related to Octel 100 Octel Analog remote machines:

- Octel 100 remote machines do not support an update by Demand Remote Push from the Message Networking system.
- Octel 100 remote machines do not send a positive message confirmation to 10-digit dial plans.
- If a message is received by an Octel 100 subscriber that was flagged as a negative confirmation, it is turned into a positive confirmation by the Octel 100 and the sender receives a positive confirmation message.
- Based on the way that the Octel 100 machine sends a future delivery message (the Octel 100 machine sends the message immediately and expects the remote machine to hold the message until time to be delivered), future delivery messages are supported only through the Message Networking system when sent to Octel 100 Octel Analog, UM Octel Analog Networking, and Aria/Serenade Octel Analog Networking remote machines.
- When recipients of messages from Octel 100 Octel Analog systems are notified that one or more components of a multimedia message cannot be delivered, the sender is not notified. The recipient is notified to contact the sender for missing components.

Aria and Serenade Octel Analog considerations

The following considerations are related to Aria and Serenade Octel Analog remote machines:

- When sending a message using a distribution list from an Aria Octel Analog remote machine to another Aria Octel Analog remote machine, the maximum number of subscribers to which the message can be sent is based on the Aria networking parameter that defines the number of attempts the Aria machine will make to deliver a message before giving up on the connection.
- Future delivery messages are supported only through the Message Networking system when sent to

Octel 100, Unified Messenger, and Aria/Serenade Octel Analog Networking remote machines. When sending future delivery messages from an Aria Octel Analog machine to any other type of end node, the message is failed by the Message Networking system and returned to the sender with a *future delivery* error type. The Message Networking system uses the time stamp it receives to determine if a message is for future delivery.

- For fax-only messages to Aria systems, "Your fax message is attached" is added as a voice component.
- The Aria Message Locator feature applies to Message Networking delivery.
- When Aria subscribers send a mixed Private or Priority message to multiple Avaya recipients on the same remote machine, the message is marked Priority or Private for all recipients, even if only one recipient is marked as such.
- When recipients of messages from Aria and Serenade Octel Analog systems are notified that one or more components of a multimedia message cannot be delivered, the sender is not notified. The recipient is notified to contact the sender for missing components.
- Reply/Forward Indicator is supported:
 - From Serenade Octel Analog Networking to all machine types.
 - From Serenade Digital to Serenade Digital.
- Serenade Digital call processing features are NOT supported (for example, Immediate Call).
- Note the use of "notice" versus "message" for Aria and Serenade systems. Historically, notices were used to indicate message delivery failure. However, when messaging using the Message Networking system:
 - "Message" indicates a failure.
 - "Notices" indicate a positive message confirmation.
- The transmission of a subscriber voiced name with a length of 8 seconds or greater is not supported when using Octel 250/350 with Octel Analog. This is a limitation of the Octel 250/350 when using Octel Analog Networking and is not specific to Message Networking.
- When you want to send a message to all subscribers in an Enterprise using a single Enterprise List, the following suggestions can help to reduce network traffic load and the effects of MWIs:
 - For Octel 250/350 servers, reference a single bulletin broadcast mailbox per server in an Enterprise List. Using this method, only one message is sent to each server. After the message is deposited in the bulletin broadcast mailbox, the message is sent to everyone on the server with the bulletin broadcast class of service (with no MWI). Use of this feature might require an Administrator to add the bulletin broadcast class of service to the subscriber on the Octel 250/350 server.
 - For Octel 200/300 servers, an Enterprise List can be created that references an Octel 200/300 System Distribution List (SDL) consisting of all local subscribers. SDLs have the option (through parameter 145) to invoke MWI or not. This scenario significantly decreases network traffic load and reduces the effects of MWI.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machines overview](#) > [Remote machine considerations](#) > Unified Messenger remote machine considerations

Unified Messenger remote machine considerations

The following are notes and considerations related to Unified Messenger remote machines:

- On Message Networking, networking is provided through Octel Analog or SMTP/MIME for Unified Messenger for Exchange Release 4.0 and 5.0.
Note: For Release 3.1 and Release 5.2, Modular Messaging/Exchange only supports Octel Analog Networking and not SMTP/MIME.
- The Microsoft Exchange Directory is used for data storage of directory updates for Unified Messenger analog remote machines. As a result of using the Microsoft Exchange Directory, there are limitations on the updates of the remote subscriber directory stored on the UM system:
 - UM does not execute a pull/update for nonexistent remote subscribers. Each remote subscriber must be preadministered as a Custom Recipient Record on the UM system for the UM system to execute a pull/update. Only the spoken name from the Message Networking system is added to the Custom Recipient Record when a UM originator sends a message to the recipient and the recipient has a recorded name for Octel Analog on the Message Networking system.
 - The Unified Messenger directory will not accept a push from the Message Networking system.
 - All remote subscriber entries are permanent (versus usage-based) on the UM.
 - UM does not support the concept of ASCII name mismatch for updating its directory. No updates, other than the first population of the spoken name in the Custom Recipient Record, are performed.
- For Unified Messenger remote machines using SMTP/MIME, there are limitations related to the remote subscriber directory updates stored on the UM system:
 - UM does not execute a pull/update for nonexistent remote subscribers. Each remote subscriber must be preadministered as a Custom Recipient Record on the UM system for the UM system to execute a pull/update.
 - When a UM sender sends a message through Message Networking, the Message Networking system updates the sender's ASCII name in its directory if it has changed from the current ASCII name for that subscriber.
 - All remote subscriber entries are permanent (versus usage-based) on the UM.
 - When a voice message is sent to a UM using Microsoft Exchange, the voice message is treated as an email message (a .wav file binary attachment) rather than a voice message.
- Only voice components are sent to a Unified Messenger user's mailbox. Faxes are dropped, and receivers hear a voice message asking them to contact the sender (Octel Analog Networking only).
- To use spoken name confirmation for messages sent from Unified Messenger through the Message Networking gateway, a custom recipient with an Octel Analog Networking address type is required for each Message Networking user in the Exchange directory.
- When recipients of messages from Unified Messenger systems are notified that one or more components of a multimedia message cannot be delivered, the sender is not notified. The recipient is notified to contact the sender for missing components.
- UM does not support private message marking using Octel Analog. This is important to note as the recipient can forward private messages sent from Message Networking to a UM recipient.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machines overview](#) > [Remote machine considerations](#) > Aria Digital and Serenade Digital remote machine considerations

Aria Digital and Serenade Digital remote machine considerations

The following are considerations related to Aria Digital and Serenade Digital remote machines:

- Announcements cannot be customized.
- For fax-only messages to Aria remote machines, the following voice component is added by the Message Networking system: "Your fax message is attached."
- Octel 200/300 message servers support multiple voice components or segments within the same message. When this type of message is sent through Message Networking, the Message Networking system concatenates all voice segments into a single component.
- Message Networking supports connectivity to a Serenade gateway when the gateway is part of an Octel 200/300 domain. Message Networking does not support a Serenade gateway when it is in a remote configuration where it is the interface for non-domain message servers:
 - A Serenade gateway in a domain configuration is an Octel 200/300 server designated as the gateway for the entire cluster of digital Octel 200/300 servers (domain). It is the only system networked to the Message Networking system within the entire domain and must be connected to all of the Octel 200/300 servers in the cluster (domain) digitally.
 - A Serenade gateway in a remote configuration is an Octel 200/300 server being used as a networking gateway for other messaging systems (connected using Octel Analog, etc.)
- In Octel 250/350 environments with alias mailboxes, when defining the dial plan, note that Message Networking delivers networked messages to the actual mailbox ID, not the alias mailbox ID. Alias mailboxes are used in Octel 250/350 systems when the call coverage number for a mailbox does not necessarily match the actual mailbox ID.
- An Octel 250/350 server that has been previously upgraded from an Aspen system and will now be used for digital networking requires that the subscribers on the system rerecord their spoken (voiced) names for the spoken name to be transmitted to the Message Networking system. In some cases, although the Octel 250/350 server was installed new, the subscriber directory was loaded from an older Aspen system. These systems must also rerecord the subscriber names. This is a limitation of the Octel 250/350 server and is not specific to Message Networking. Message Networking does not support Aspen systems. Aspen servers must first be upgraded to Octel 250/350 servers before networking to Message Networking (preferably using Aria TCP/IP).
- For an Octel 250/350 message server to use digital networking with Message Networking, it must be Release 2.05 or later. This version allows administrators to set a flag automatically requesting subscribers in the upgraded system to rerecord their spoken names. It is recommended that this flag be set several weeks before the digital connection is made to the Message Networking system to "clean out" nonconforming names.
- Due to an issue with how Aria Digital systems send out subscriber ASCII names, Octel 250/350 Release 3.0 is not supported for Message Networking. Customers with Octel 250/350 must upgrade their systems to Release 3.01.
- The Aria Message Locator feature applies to Message Networking delivery.
- Aria Digital subscribers with no recorded spoken name are sent to Message Networking upon the demand execution of an Aria NameSend. However, a new subscriber added to an Aria Digital system for whom a spoken name has not been recorded is not sent to Message Networking as an add until a spoken name is recorded.
- Large messages to AUDIX from Aria and Serenade are failed with a *message length* failure message.
Note: AUDIX LX supports voice messages of up to 180 minutes.

- When Aria senders send a mixed private and/or priority message to multiple Serenade or VPIM V2 digital recipients on the same remote machine, the message is marked Priority and/or Private for all recipients, even if one recipient is marked as such. The sender is not notified that this has happened.
- Reply/Forward Indicator is supported:
 - From Serenade Octel Analog Networking to all machine types
 - From Serenade Digital to Serenade Digital
- Serenade Digital call processing features (for example, Immediate Call, Check for Unlistened Messages) are *not* supported.
- When recipients of messages from Aria Digital and Serenade Digital systems are notified that one or more components of a multimedia message cannot be delivered, the sender is not notified. The recipient is notified to contact the sender for missing components.
- Note the use of "notice" versus "message" for Aria and Serenade systems. Historically, notices were used to indicate message delivery failure. However, when messaging using the Message Networking:
 - "Message" indicates a failure.
 - "Notices" indicate a positive message confirmation.
- One message for multiple recipients is supported; each recipient receives header information (private, priority, AND confirmation request).
- Subscriber updates are supported as follows:
 - Automatic on add, change, and delete (no delete for Serenade Digital).
 - Automatic on message delivery to a recipient (updates recipient).
- The transmission of a subscriber spoken name with a length of eight seconds or greater is not supported when using Octel 250/350 with Octel Analog Networking. This is supported for all other remote machine and protocol types, including Aria Digital TCP/IP.
- Self-registration is not supported for Aria/Serenade Digital; NameSend is used instead.
- The default value of Octel serial number for Message Networking is 80000 (range of 80000 to 81000 reserved).
- A maximum of 1 outbound port per remote machine, rounded up, is supported.
- The following features are *not* supported:
 - Multiple inbound simultaneous sessions from a given remote machine.
 - Multiple outbound simultaneous sessions to a given remote machine.
 - Network turnaround.
- Sender's Name:
 - Octel messages, Aria Digital messages, and Serenade Digital messages to Message Networking need to be configured to exclude the Sender's Name Prefix.
 - Octel Analog Networking, Aria Digital, Serenade Digital, and AMIS recipients receive the sender's name by using Message Networking prefixing.
 - AUDIX recipients receive the sender's name from the message header.
- In some Dial Plans, the Message Networking system needs to build back the complete address of the sender (including prefix) before transmitting to a Serenade Digital machine. For example, if the Serenade Digital machine attaches a prefix of 1 before the 10-digit network address to a recipient, then the Message Networking system must be configured to attach the same prefix of 1 before that sender's 10-digit network address when the recipient replies to the Serenade Digital machine. In this case, Message Networking supports creation of a [Serenade Digital Sender Dial Plan](#).
- Serenade Digital remote machines do not support analog fallback on outbound or inbound messages.
- The 3/4 Rule is supported for Serenade Digital remote machines for inbound and outbound ports:

- No more than 3/4 of all Serenade Digital ports can be used for outbound.
- No more than 3/4 of all Serenade Digital ports can be used for inbound.
- Numbers are rounded up.
- No ports are reserved for inbound or outbound if ports total 1, 2, or 3.
- When you want to send a message to all subscribers in an Enterprise using a single Enterprise List, the following suggestions can help to reduce network traffic load and the effects of MWIs:
 - For Octel 250/350 servers, reference a single bulletin broadcast mailbox per server in an Enterprise List. Using this method, only one message is sent to each server. After the message is deposited in the bulletin broadcast mailbox, the message is sent to everyone on the server with the bulletin broadcast class of service (with no MWI). Use of this feature might require an Administrator to add the bulletin broadcast class of service to the subscriber on the Octel 250/350 server.
 - For Octel 200/300 servers, an Enterprise List can be created that references an Octel 200/300 System Distribution List (SDL) consisting of all local subscribers. SDLs have the option (through parameter 145) to invoke MWI or not. This scenario significantly decreases network traffic load and reduces the effects of MWI.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machines overview](#) > [Remote machine considerations](#) > VPIM remote machine considerations

VPIM remote machine considerations

Consideration the following when you administer VPIM V2 remote machines:

- Depending on the implementation of VPIMv2, some of the feature interactions might differ from one vendor to another. Also, when the remote VPIM system type is not the one which Avaya has previously tested, customer may request Avaya and the third party VPIM vendor to assist in testing.
- When the VPIM V2 message sent is larger than what a non-VPIM machine can handle, the system fails to deliver and displays "Large Message" error message.
- When recipients of messages from VPIM V2 systems are notified that one or more components of a multimedia message cannot be delivered, the sender is not notified. However, the recipient is notified to contact the sender for missing components.
- VPIM machine type supports the VPIM V2 protocol. However, the message exchange happens only through standard SMTP and does not support secure SMTP.
- VPIM V2 does not support sending a new, update, or delete either inbound or outbound message when a subscriber record has been updated by an Administrator.
- The maximum number of recipients per message on an inbound VPIM V2 message is 1,000. The maximum number of recipients per message on an outbound VPIM message is 250.
- VPIM V2 remote machines administered on the Message Networking system support only dynamic directory views. This means that the Message Networking system sends subscriber directory updates to a VPIM V2 remote machine as subscribers send messages to that VPIM V2 machine.
- VPIM V2 does not support the following combinations for future delivery: Aria/Octel 100/UM to AUDIX/AMIS/Serenade Digital/VPIM V2.
- Sender notification of message receipt is handled in one of the following ways:
 - An originator sending a message from a VPIM V2 remote machine to a non-VPIM remote machine does not get an indication that the recipient has accessed the message.
 - An originator sending a message from a non-VPIM remote machine to a VPIM V2 remote machine does not get an indication that the recipient has accessed the message. Requests for this information are ignored.
 - An originator sending a message from a VPIM V2 remote machine also supporting the accessed feature gets an indication that the recipient has accessed the message. This response is in text format.
- Message Disposition Notification (MDN) is handled in one of the following ways:
 - For messages sent from VPIM remote machines to non-VPIM remote machines, Message Networking ignores MDN requests.
 - For messages sent from VPIM to VPIM remote machines, Message Networking returns whatever the receiving VPIM machine returns, for example, MDN, "Ignore," and so on.
- VPIM v2 systems do not support negative confirmation.
- Demand Remote Update and Demand Remote Push do not apply to VPIM systems.
- Disabling of Updates In or Out does not apply to VPIM v2 systems.
- VPIM V2 subscriber records can be imported using the FTP subscriber import utility.
- Message Networking follows a default transmission schedule for message delivery to VPIM remote

machines. This schedule defaults to all hours (00:00-23:59). An immediate trigger for VPIM message delivery occurs when a message for a given remote VPIM machine is placed on the queue. All messages on the queue for that remote VPIM machine are sent during the same communication session for that remote machine. This schedule is not tunable.

- Message Networking provides the ability to administer up to three Domain Name Servers (DNSs) to be used (in priority order) when the VPIM module needs to locate the IP address necessary to communicate with the appropriate VPIM message server. When configuring a VPIM remote machine domain, the use of a DNS is optional. In cases where DNS is not used, the IP address for the VPIM domain being configured must be specified.
- The Message Networking system requires a uniform length dial plan (the number of digits used when addressing a message). It consists of a network address of from 3 to 10 digits. A 10-digit network address dial plan is recommended.
- *Delivered* status indicates the message was delivered to the Message Networking system. If a message fails, the original message is returned, and two messages are returned to the sender's incoming mailbox:
 - An error message similar to:
"Message to [voice name(s)] extension [extension number(s)] failed due to [reason]. A copy of this message can be found in your incoming mailbox."
This error message might have Priority status if this option was selected through the administration pages.
 - The actual message is returned to the sender so that it can be resent to the destination.
- A recipient of a message must be administered on a Message Networking system in order for that Message Networking system to accept messages for delivery.
- Notification of failure to deliver a message component because the recipient is not enabled to receive a component type (voice, fax, text, binary) is the same as on the INTUITY AUDIX Release 4 system. The component that could not be delivered is stripped, and the following statement is prefixed to the original message: "One or more components could not be delivered, please contact the sender" <pause><voice message>.
- Octel Analog Networking analog subscriber messages can optionally contain the Private/Urgent designation and voiced name of the sender as part of the actual message being sent.
- The remote subscriber name contains a suffix indicating the Message Networking system ID for the remote machine on which that subscriber resides.
Note: This suffix can take from 2 to 8 characters at the end of the Name field.
- When the Message Networking database is full, subscribers continue to be added but voiced names are not. Therefore, no voiced name is heard when addressing a subscriber whose voiced name could not be added. Message Networking supports 120,000 subscribers with voiced names.
- Sender's name:
 - Octel Analog Networking, Aria Digital, and Serenade Digital messages to Message Networking should not be configured to include the sender's name.
 - Octel Analog Networking, Aria Digital, and AMIS recipients receive the sender's name by Message Networking prefixing.
 - AUDIX and Serenade Digital recipients receive the sender's name from the message.
- Message Networking supports a maximum mailbox ID and network address length of 10 digits and a minimum mailbox ID length of 3 digits. In addition, Message Networking supports a uniform dial plan whereby the network address length must be the same number of digits network-wide (from 3 to 10 digits). None of the Avaya message servers that Message Networking supports can have a mailbox ID or network address greater than 10 digits. Additionally, it is expected that every Message Networking system with a VPIM connection have at least one Avaya message server in its network. The VPIM specification recommends (but does not require) E.164 conformance for the format of the userid@domain address. This specification calls for a userid value length of up to 30 digits and/or characters.
- The Message Networking VPIM module does not support network turnaround, as this is not a feature of the VPIM protocol.

- Message Networking does not support the disabling of Updates In or Out for VPIM remote machines, as this concept does not apply to VPIM.
- Message Networking does not support the ability to change a remote machine administered as AMIS type to VPIM. The remote AMIS machine must be deleted and readministered as a VPIM remote machine on the Message Networking system.
- Messages delivered to VPIM recipients from Message Networking include the sender's voiced and ASCII names in the appropriate sender's name fields. For the voiced name, the ADPCM format is used if the voiced name is stored on the Message Networking system. How the names are presented to the recipient (if at all) depends on the receiving VPIM vendor's implementation. For example, Message Networking sends a voiced name to some vendors that ignore this field and do not present it to the recipient. For inbound VPIM messages received, Message Networking extracts the sender's voiced and ASCII names from the appropriate sender's name fields and populates the Message Networking directory accordingly. It is important that VPIM customers verify the level of name support on the vendor's VPIM system that is planned to be networked to the Message Networking system. In short, Message Networking supports both the ASCII and voiced name values in its VPIM implementation, but it is the individual VPIM vendor's support of these that can affect the user experience.
- Message Networking's VPIM implementation supports voice, fax, and text components of a message. However, certain vendors have chosen not to support fax and text in their VPIM implementations. It is important that VPIM customers verify the level of component support in the vendor's VPIM system that is planned to be networked to the Message Networking system.
- Certain sending VPIM systems can generate what is known as a multistrip fax, which is not supported by Message Networking. A multistrip fax is a fax with one or more pages each stored as multiple strips of image data. An example of a system that can generate a multistrip fax is Microsoft Exchange 2000.
- When a VPIM originator sends a message to a VPIM recipient through the Message Networking system (whether one or two Message Networking systems are involved), the message component handling is always a binary-to-binary mapping (that is, the original MIME format). When a VPIM originator sends a message to a non-VPIM recipient, the voice, fax, and text components are placed into the appropriate designated components for AUDIX, AMIS, Octel Analog, Aria Digital, and Serenade Digital recipients. For each component type, its sending VPIM binary representation is removed from the MIME format and placed into the receiving machine type representation. Since these receiving machine types (AUDIX, AMIS, Octel Analog, Aria Digital, Serenade Digital systems) can only support one component of each type, similar component types (voice and text) are concatenated. For fax, subsequent faxes are added as a binary attachment on the outgoing message. For INTUITY AUDIX systems, the subsequent faxes are received as a binary attachment. Because the other system types (DEFINITY AUDIX, AUDIX R1, AMIS, Octel Analog, Aria Digital, Serenade Digital) cannot handle binary or text, these components are stripped.
- Some VPIM messaging systems support a reply-all capability upon receipt of a message. However, when a message originates from a non-VPIM sender through Message Networking, the reply-all feature for the VPIM recipient is not supported. Depending on the consistency of the dial plan, messages sent from a VPIM sender to a VPIM recipient through the Message Networking system may or may not be able to perform a reply-all on the message.
Note: This consideration is not related to the reply-all feature of Message Networking's Enterprise List application, supported on the S3500-H or S8800 2U server.
- The use of DNS on Message Networking for remote VPIM domain IP resolution is optional. However, other vendors' VPIM systems might require DNS to operate. The customer must verify whether the non-Avaya VPIM messaging system requires DNS and whether the facilities exist to do this before networking the system to the Message Networking system.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machines overview](#) > [Remote machine considerations](#) > SMTP/MIME remote machine general considerations

SMTP/MIME remote machine general considerations

This topic provides information on general considerations related to SMTP/MIME remote machines.

Note: For specific considerations related to Modular Messaging and Avaya Aura™ Messaging systems that use SMTP/MIME, see [Modular Messaging remote machine considerations](#), and [Avaya Aura™ Messaging remote considerations](#).

The following are general considerations related to SMTP/MIME remote machines:

- The following are standard methods of encoding audio messages in a compressed format. Message Networking can directly process audio files of these types when they are received as .wav files that are part of an SMTP/MIME message:
 - **GSM:** In the Windows Sound Recorder, this file type has an audio format of GSM 6.10 8.000 kHz, Mono.
 - **A-law:** In the Windows Sound Recorder, this file type has an audio format of CCITT A-Law 8.000 kHz, 8 Bit, Mono.
 - **Mu-law:** In the Windows Sound Recorder, this file type has an audio format of CCITT u-Law 8.000 kHz, 8 Bit, Mono.
- In cases where a sent SMTP/MIME message is larger than a receiving non-SMTP/MIME machine can handle, the message is failed with a *large message* failure code.
- Message Networking does not support Group 4 fax transcoding.
- The Message Networking VPIM module does not support variable-length mailbox IDs on the same SMTP/MIME mail server.
- Message Networking supports a maximum mailbox ID of 30 and network address length of 10. In addition, Message Networking supports a uniform dial plan whereby the length of the network address must be the same number of digits (from 3 to 10) network-wide. None of the Avaya message servers (remote machines) that Message Networking supports can have a mailbox ID of 30 or network address greater than 10 digits. However, Message Networking does support variable-length addressing for Modular Messaging systems. Therefore, numeric addresses can be administered on Message Networking for subscribers on non-Modular Messaging and Avaya Aura™ Messaging remote machines. If you do not administer numeric address mapping, note that Message Networking supports E.164 conformance addressing from SMTP/MIME senders in the format of user id@domain. The user ID is alphanumeric and can be greater than 10 in length. Message Networking can then take this address and map it to a network address whose length cannot exceed 10.
- Certain sending SMTP/MIME systems can generate what is known as a multistrip fax that Message Networking does not support. Specifically, a multistrip fax is a fax with one or more pages each stored as multiple strips of image data. An example of a system that can generate a multistrip fax is Microsoft Exchange 2000.
- Message Networking does not support the ability to change a remote machine administered as AMIS or Octel Analog (such as Unified Messenger with MS Exchange) to SMTP/MIME. The remote AMIS/Octel Analog machine must be deleted and readministered as an SMTP/MIME remote machine on the Message Networking system.
- Virus detection and virus detection software are server-specific. Fortunately, virus infection is generally limited to binary attachments intended to execute in a PC environment. Current Avaya message servers that support binary files do not attempt to run any binary attachments on the server, so the risk of infection occurs only in the client environment. There is NO virus detection support on Message Networking. Virus detection support should be applied at the binary file detach operation on the client.

Because Message Networking is provisioned as an email receiver, customers must ensure that a firewall exists between Message Networking and the Internet. In addition, customers should deploy a virus detection solution, such as a standalone server that sits on the LAN between the Message Networking server and any incoming email. This kind of solution adds an extra transmission, but filters out viruses from incoming email. Most large corporations are already running a similar service at their publicly accessible incoming email gateway. See [Virus and worm protection](#) for more information on protecting the remote messaging system.

- If SMTP messages being sent via a sound card have static, check the users' microphone settings. You might need to adjust the microphone settings.
- Note the following considerations for voiced and ASCII names on non-LDAP-based systems:
 - Messages delivered to SMTP/MIME recipients from Message Networking include the ASCII name, but not the voiced name, in the appropriate sender's name field. How the names are presented to the recipient (if at all) depends on the receiving SMTP/MIME vendor's implementation. When the ASCII name is received by Message Networking, that sender's directory entry is updated, if necessary.
 - Message Networking can register the SMTP/MIME subscriber's voiced name in the directory using the Self-Registration Agent feature. Once recorded on the Message Networking system, the voiced name can then be presented to the rest of the network.

These considerations do not apply to Avaya Modular Messaging and Avaya Aura™ Messaging systems because they use LDAP-based utilities for subscriber directory updates, which occur automatically (similar to AUDIX TCP/IP and including ASCII and voiced name).

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machines overview](#) > [Remote machine considerations](#) > Modular Messaging remote machine considerations

Modular Messaging remote machine considerations

The following are considerations related to Modular Messaging remote machines.

General Modular Messaging/MSS considerations

The following are general Modular Messaging/Avaya Message Store (MSS) system considerations:

- LDAP updates (between Modular Messaging, and Message Networking systems and between multiple Message Networking systems) can impact system performance, including delay of administration page displays and report results. Note that while the LDAP update is in progress between the two systems, messages are not transmitted between them. The length of time to complete an LDAP update depends on:
 - The type of Modular Messaging systems (Standard or High Availability)
 - The number of MASs in the system
 - The size of the system's database
 - The number of subscribers to be updated and the voice name message lengths
 - The number of updates occurring at the same time (multiple updates running slow the update rate)

Avaya recommends that you run remote updates of more than approximately 4,000 subscribers with voiced names during non-prime-time hours, and that you run remote updates of 50,000 subscribers or more over a weekend.

For Modular Messaging systems updates, Standard Availability systems and systems with multiple MASs will take longer to update. The following approximate update rates are provided to help estimate the total time required for a remote update of a Modular Messaging systems:

- For a Modular Messaging Release 3.1 system on a S3500-H (High Availability) with one MAS, the update rate is 9,000 subscribers per hour. Depending on your system configuration and system activity, this update might complete faster.
- For a Modular Messaging Release 5.x systems on an S8800 2U server with one MAS, the update rate is 9,000 subscribers per hour. Depending on your system configuration and system activity, this update might complete faster.

Note: To expedite Modular Messaging system updates, Avaya recommends that you first set the **Log Updates In** field to **no** on the **Edit Networked Machine** page of the Modular Messaging systems.

- For Message Networking to Message Networking updates, the following approximate update rates apply:
 - For a Message Networking Release 2.0 system on an S3210R server, the update rate is 5,000 to 7,000 subscribers per hour.
 - For a Message Networking Release 3.1 system on an S3210R server, the update rate is 5,000 to 7,000 subscribers per hour.
 - For a Message Networking Release 3.1 system on an S3500-H server, the update rate is 14,000 to 15,000 subscribers per hour. Depending on your system configuration and system activity, this update might complete faster.
 - For a Message Networking Release 5.2 system on an S3500 Basic server, the update rate is 5,000 to 7,000 subscribers per hour.
 - For a Message Networking Release 5.2 system on an S8800 2U server, the update rate is 14,000

to 15,000 subscribers per hour. Depending on your system configuration and system activity, this update might complete faster.

- When administering multiple Modular Messaging systems in a network, there are two scenarios for directory updates:
 - Each Modular Messaging system provides updates directly to the other Modular Messaging systems in the network.
 - Message Networking provides the updates to the Modular Messaging systems in the network.

There are [considerations](#) for each scenario that you must be aware of before administering the Modular Messaging systems:

- Modular Messaging systems do not accept more than 250,000 subscribers (with or without voice names) during an update. Therefore, if the Message Networking system has more than 250,000 subscribers, you must [administer the Modular Messaging remote machines](#) to use directory view updates, and the [directory view](#) you administer for the Modular Messaging systems must include no more than 250,000 subscribers.
- When setting up an email client such as Outlook Express for use with Avaya Modular Messaging, you must provide an email address for each subscriber. There are two ways that you can specify email addresses on the Avaya Modular Messaging system:
 - Mailbox number (which is also used in the Account Name field in the Outlook Express administration setup) combined with the domain of the Avaya Modular Messaging (for example, 5553530@mm.avaya.com).
 - ASCII name email address (for example, Joe.Smith@mm.avaya.com).

However, to send messages from an Avaya Modular Messaging mailbox through Message Networking, the subscriber's email address in Outlook Express must match the subscriber's ASCII name email address.

- Replies to messages originating from an Avaya Modular Messaging systems Enhanced List Application are not supported when the message is passed through a Message Networking system. The only way for the recipient to reply to the sender is to forward the message back to the originator.

Note: This consideration is not related to the reply-all feature of Message Networking's Enterprise List application, supported on the S8800 2U server, which does support reply-all regardless of the sender or originator type.

- Avaya Modular Messaging supports a reply-all capability when messages are exchanged between Modular Messaging subscribers. However, the reply-all capability is not supported for messages originating from non-Modular-Messaging senders that are passed through Message Networking.

Note: This consideration is not related to the reply-all feature of Message Networking's Enterprise List application, supported on the S8800 2U server, which does support reply-all regardless of the sender or originator type.

- Avaya Modular Messaging Release 2.0 systems do not support private message marking when sending or receiving a networked message. This is important to note as a recipient can forward private messages sent from Message Networking to a another recipient. Priority message markings are supported.
- The length of the Numeric Address for a Modular Messaging subscriber cannot be the same length as the Mailbox ID value for a subscriber when those subscribers are in the same Voice Mail Domain. The numeric Network Address value can, however, be the same length. This is important to note when the customer is planning the numeric dial plan for the network.
- Modular Messaging allows a recipient of a message to call the sender of a networked message. The dial plan to call the sender must match the sender value used when the message is delivered. It is important to plan for the Mailbox ID length, Numeric Address length, and Network Address length when designing a network that involves Modular Messaging and Message Networking.
- With the Reply to Call Answer Message feature in Modular Messaging, a recipient of a call answer message can reply back to the caller using Message Networking only when both the caller and recipient are in the same Voice Mail Domain.

Considerations for Modular Messaging/MSS using SMTP/MIME

There are several considerations when using SMTP/MIME as the message delivery mechanism to Modular Messaging with an Avaya Message Storage Server (MSS):

- When a message is sent through Message Networking to a subscriber with a full mailbox on a Modular Messaging/MSS system, the time it takes for the failure notification to be sent from Modular Messaging to Message Networking depends on the delivery attempts setting on Modular Messaging systems. The higher the number of retries, the longer it takes for the failure notification to be sent to the sender.
- When a message is sent through Message Networking to a nonexistent subscriber on a Modular Messaging/MSS system, Modular Messaging notifies Message Networking immediately. Message Networking sends the failure notification to the sender when the next poll occurs.
- When multiple Modular Messaging systems using MSSs are installed in a network, a Message Networking system might be recommended to ease system administration or improve directory update performance. Message Networking eases administration by eliminating the need to administer every machine in the network on each Modular Messaging systems. Instead, all machines are administered on the Message Networking and each Modular Messaging machines need only administer the Message Networking system. Large directory updates between Modular Messaging systems can significantly impact system performance. Message Networking improves performance of directory updates by eliminating the possibility of multiple directory updates occurring at the same time. MSS-H improves performance of directory updates by providing higher throughput than MSS-S.

Whether a Message Networking system is required depends on the number of Modular Messaging systems and the number of subscribers on each Modular Messaging system. The following table identifies when a Message Networking is required.

Average # of MM subscribers	Number of MM systems with an MSS		
	2 to 5	5 to 10	More than 10
Less than 200	Optional	Optional	Recommended for administration
200–2,000	Optional	Optional	Recommended for administration and performance
2,000–5,000	Optional	Recommended for performance	Recommended for administration and performance
5,000–10,000 (recommend MSS-H for Modular Messaging)	Recommended for performance	Recommended for performance	Strongly recommended for administration and performance
More than 10,000 (strongly recommend MSS-H for Modular Messaging)	Strongly recommended for performance	Strongly recommended for performance	Strongly recommended for administration and performance

Considerations for Modular Messaging/Exchange using Octel Analog Networking

The following considerations are specific to Modular Messaging with Exchange systems using Octel Analog Networking.

Modular Messaging/Exchange Directory Updates using Octel Analog Networking

Modular Messaging/Exchange uses Microsoft Exchange's directory. As a result, there are certain limitations relative to the updates of the remote subscriber directory stored on the Modular Messaging systems. These limitations include:

- Message Networking can pull updates from Modular Messaging/Exchange systems for administered local subscribers. See the Avaya Modular Messaging for Microsoft Exchange Installation for information on administering local subscribers on Modular Messaging/Exchange systems.
- Modular Messaging/Exchange do not execute a pull/update for non-existent remote subscribers. All remote subscribers must be preadministered as a Custom Recipient Record on the Modular Messaging/Exchange systems for Modular Messaging/Exchange softwares to execute a pull/update. Only the spoken name from the Message Networking solution is added to this record when a Modular Messaging/Exchange originator sends a message to the Custom Recipient and the recipient has a recorded name on the Message Networking solution.
- Modular Messaging/Exchange do not support the concept of ASCII name mismatch for updating its directory (this feature is used by other Octel® Analog Networking systems). No updates, other than the first population of the spoken name in the Custom Recipient Record, are performed.
- No subscriber pushes/updates are accepted from Message Networking.
- All remote subscriber entries are permanent (versus usage-based) on the Modular Messaging/Exchange solution.

These are directory limitations of Modular Messaging/Exchange and not the Message Networking implementation of Octel Analog Networking. Component types such as text and binary are not supported in Modular Messaging/Exchange using Octel Analog Networking as a transport. Modular Messaging/Exchange systems require a separate fax server to support fax components

Note: For Release 5.x, Modular Messaging/Exchange only supports Octel Analog Networking and not SMTP/MIME.

Modular Messaging/Exchange Directory Updates using Octel Analog Networking for Message Delivery

Modular Messaging/Exchange uses Microsoft Exchange's directory, and, as a result, has certain limitations relative to the updates of the remote subscriber directory stored on the Modular Messaging/Exchange systems. These limitations include:

- The Modular Messaging/Exchange solutions do not execute a pull/update for remote subscribers. All remote subscribers must be preadministered as a Custom Recipient Record on the Modular Messaging/Exchange systems.
- When a Modular Messaging/Exchange sender sends a message through the Message Networking solution, the Message Networking solution updates the sender's ASCII name in its directory if it has changed from the current ASCII name for that subscriber.
- All remote subscriber entries are permanent (versus usage-based) on the Modular Messaging/Exchange solution.

Note: For Release 5.x, Modular Messaging/Exchange only supports Octel Analog Networking and not SMTP/MIME.

Private messages

Modular Messaging/Exchange do not support private message marking using Octel Analog Networking. This is important to note as the recipient can forward private messages sent from Message Networking to a Modular Messaging with Exchange Directory Updates using Octel Analog Networking for Message Delivery/Exchange recipient. Priority message markings are supported.

Modular Messaging/Domino considerations

For Release 5.x, Modular Messaging/Domino is not supported with Message Networking.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Remote machines overview](#) > [Remote machine considerations](#) > Avaya Aura™ Messaging remote machine considerations

Avaya Aura™ Messaging remote machine considerations

The following are considerations related to Avaya Aura™ Messaging remote machines.

General Avaya Aura™ Messaging considerations

The following are general Avaya Aura™ Messaging system considerations:

- LDAP updates (between Avaya Aura™ Messaging and Message Networking systems and between multiple Message Networking systems) can impact system performance, including delay of administration page displays and report results. Note that while the LDAP update is in progress between the two systems, messages are not transmitted between them. The length of time to complete an LDAP update depends on:
 - The size of the system's database
 - The number of subscribers to be updated and the voice name message lengths
 - The number of updates occurring at the same time (multiple updates running slow the update rate)

Avaya recommends that you run remote updates of more than approximately 4,000 subscribers with voiced names during non-prime-time hours, and that you run remote updates of 50,000 subscribers or more over a weekend.

Note: To expedite Avaya Aura™ Messaging system updates, Avaya recommends that you first set the **Log Updates In** field to **no** on the **Edit Networked Machine** page of the Avaya Aura™ Messaging systems.

- When administering multiple Avaya Aura™ Messaging systems in a network, there are two scenarios for directory updates:
 - Each Avaya Aura™ Messaging system provides updates directly to the other Avaya Aura™ Messaging systems in the network.
 - Message Networking provides the updates to the Avaya Aura™ Messaging systems in the network.

There are [considerations](#) for each scenario that you must be aware of before administering the Avaya Aura™ Messaging systems:

- Avaya Aura™ Messaging systems do not accept more than 250,000 subscribers (with or without voice names) during an update. Therefore, if the Message Networking system has more than 250,000 subscribers, you must [administer the Avaya Aura™ Messaging remote machines](#) to use directory view updates, and the [directory view](#) you administer for the Avaya Aura™ Messaging systems must include no more than 250,000 subscribers.

Considerations for Avaya Aura™ Messaging using SMTP/MIME

There are several considerations when using SMTP/MIME as the message delivery mechanism to Avaya Aura™ Messaging:

- When a message is sent through Message Networking to a subscriber with a full mailbox on a Avaya Aura™ Messaging system, the time it takes for the failure notification to be sent from Avaya Aura™ Messaging to Message Networking depends on the delivery attempts setting on Avaya Aura™ Messaging systems. The higher the number of retries, the longer it takes for the failure notification to be sent to the sender.

- When a message is sent through Message Networking to a nonexistent subscriber on a Avaya Aura™ Messaging system, Avaya Aura™ Messaging notifies Message Networking immediately. Message Networking sends the failure notification to the sender when the next poll occurs.
- When multiple Avaya Aura™ Messaging systems are installed in a network, a Message Networking system might be recommended to ease system administration or improve directory update performance. Message Networking eases administration by eliminating the need to administer every machine in the network on each Avaya Aura™ Messaging systems. Instead, all machines are administered on the Message Networking and each Avaya Aura™ Messaging machines need only administer the Message Networking system. Large directory updates between Avaya Aura™ Messaging systems can significantly impact system performance. Message Networking improves performance of directory updates by eliminating the possibility of multiple directory updates occurring at the same time.

Whether a Message Networking system is required depends on the number of Avaya Aura™ Messaging systems and the number of subscribers on each Avaya Aura™ Messaging system. The following table identifies when a Message Networking is required.

Average # of Avaya Aura™ Messaging subscribers	Number of Avaya Aura™ Messaging systems		
	2 to 5	5 to 10	More than 10
Less than 200	Optional	Optional	Recommended for administration
200–2,000	Optional	Optional	Recommended for administration and performance
2,000–5,000	Optional	Recommended for performance	Recommended for administration and performance
5,000–10,000	Recommended for performance	Recommended for performance	Strongly recommended for administration and performance
More than 10,000	Strongly recommended for performance	Strongly recommended for performance	Strongly recommended for administration and performance

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Administration](#) > [Administering remote machines](#) > [Adding remote machines](#) > Adding an Adding an Avaya Aura™ Messaging remote machine

Adding an Avaya Aura™ Messaging remote machine

This topic provides information on adding an Avaya Aura™ Messaging remote machine to the Message Networking system.

Note: The checklist for adding an Avaya Aura™ Messaging remote machine provides a list of steps you must complete when adding a new Avaya Aura™ Messaging remote machine to the Message Networking system.

To add an Avaya Aura™ Messaging remote machine:

1. Start at the Administration menu, and select **MN Administration > Remote Machines > Add a Remote Machine**.
The system displays the **Add a New Machine** page.
2. Type a name for the new machine in the **New Machine Name** field, and then click **Next Step**. For information on [valid machine names](#), click the field name or **Help** on the Web-based administration page.

A **Machine Type** field appears on the page.

3. Select **Avaya Messaging Multisite** from the **Machine Type** menu.
The **Bridged Machine?** and **IP Address** fields appear on the page.

Note: The **Bridged Machine?** field does not appear if the Number of Bridged Machines on the [Customer Options page](#) is set to 500 (the maximum).

4. In the **Bridged Machine?** field, specify whether this remote machine is a bridged machine. For information on [bridged machines](#), click the field name or **Help** on the Web-based administration page.
5. In the **IP Address** field, you can optionally type the IP address of the remote machine you are creating. For information on [valid IP addresses](#), click the field name or **Help** on the Web-based administration page.
6. Click **Next Step**.
The remote machine parameter fields display on the page.
7. [Complete the remote machine parameter fields](#). For information on completing the fields, click the field names or **Help** on the Web-based administration page.
8. Click **Next Step**.
The administration fields display on the page.
9. [Complete the administration fields](#). For information on completing the fields, click the field names or **Help** on the Web-based administration page.
10. Click **Next Step** to save the remote machine and [administer Dial Plan Mapping](#), or click **Add this Machine** if you do not want to administer Dial Plan Mapping at this time:
 - If you click **Next Step**, the system displays the **Dial Plan Mapping** page.
 - If you click **Add this Machine**, the system displays a message that the parameters have been saved. Click **OK**.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Administration](#) > [Administering remote machines](#) > [Checklists for administering new remote machines](#) > Checklist for adding a new Avaya Aura™ Messaging remote machine



Checklist for adding a new Avaya Aura™ Messaging remote machine

The following table lists the procedures for adding a new Avaya Aura™ Messaging machine to the Message Networking system. The procedures appear in the sequence in which they are performed.

Some of these tasks require you to access the Avaya Aura™ Messaging system. If you are unfamiliar with Avaya Aura™ Messaging, ask the Avaya Aura™ Messaging system administrator to assist you.

Completed	Task
	<p>Gather the information that you may need when you later administer the dial plan mapping on the Message Networking system.</p> <p>Obtain the Network Address Length from the General Parameters page on the Message Networking system. This number represents the specific number of digits, usually 7 or 10, required for messages to be sent through the Message Networking system. Generally, the network address consists of the dial plan mapping plus the extension. Usually, for your dial plan mapping, you use the same area code and local exchange (DID) used to reach the Avaya Aura™ Messaging subscribers through the PBX. You can obtain the area code and local exchange from the switch administrator. You also need to obtain the extension ranges for the Avaya Aura™ Messaging system. You can obtain these ranges from the Avaya Aura™ Messaging system administrator</p> <p>For example, for a system requiring 10-digit dialing, mailboxes in the range 20000 to 29999 might normally be preceded by 555-12. If an outside caller wants to leave a message for mailbox 20001, the caller needs to dial 555-122-0001. This same number can be used to create the network address. In this case, 55512 is the dial plan mapping on the Message Networking system and 20001 is the 5-digit Avaya Aura™ Messaging extension. This example assumes that the network address requires 10-digit dialing.</p> <p>However, it is possible in a 7-digit or 10-digit dialing area that different ranges on the new system could be preceded by different dial plan mapping. Therefore, although some mailboxes are preceded by 555-12, a different extension range 50000 to 59999 might be preceded by 555-34. In this case, an outside caller would dial 555-345-0002 to call mailbox 50002. These numbers can also be used to create the network addresses. In this example, to create the network address on the Message Networking system, you can add a Dial Plan mapping for this remote machine where, for mailbox ranges 50000 to 59999, you administer a Map To of 55534. This configuration adds 55534 to the mailbox IDs in the specified range to create the 10-digit network addresses.</p>
	<p>On the Message Networking system:</p> <p>Gather the information about the Message Networking system that you may need when administering the Message Networking system on the</p>

	<p>Avaya Aura™ Messaging system:</p> <p>On the General Parameters page:</p> <ul style="list-style-type: none"> • Record the Local Machine Name. • Record the IP address from the Local Machine IP Address field. • Record the password in the LDAP Password field. • Record the number of digits in the Network Address Length field. <p>If this is a new Message Networking system and the fields on the General Parameters page are not yet completed, you must administer the General Parameters page before continuing.</p>
	<p>On the Avaya Aura™ Messaging system: From the Avaya Aura™ Messaging administration, obtain a specific mailbox ID on the Avaya Aura™ Messaging system that receives and sends a test message through Message Networking.</p> <p>Message Networking allows assignment of multiple mailbox number lengths for Serenade Digital (SDG), Serenade Octel Analog (SOAN), Avaya Modular Messaging MultiSite and Avaya Aura™ Messaging remote machines. This allows all the mailboxes on a remote machine that has variable length mailboxes to communicate with the Message Networking system to exchange messages and subscriber information. For example, if a remote machine has both 4-digit and 5-digit mailboxes, the mailboxes can send and receive messages from the Message Networking system. Each of the mailbox number lengths is restricted to be between 3 and 30 for an Avaya Aura™ Messaging system. However, duplicate mailbox number lengths are disallowed. For remote machines other than SDG,SOAN, Avaya Modular Messaging MultiSite and Avaya Aura™ Messaging you must administer a dial plan with single length mailboxes in order for the mailboxes to communicate with the Message Networking system.</p> <p>Note: Because every Message Networking address must be unique, there might be circumstances in which the new system's mailbox ID length matches the Message Networking dial plan, but because the new system is not part of the same switch private network, the mailbox IDs might not be unique within the Message Networking network. This situation is common, which is why it is normally recommended to use a 10-digit Message Networking dial plan and dial plan mapping.</p>
	<p>On the Avaya Aura™ Messaging system:</p> <p>Administer the Messaging Networking system as a networked machine on the Avaya Aura™ Messaging system:</p> <ol style="list-style-type: none"> 1. After logging into the Avaya Aura™ Messaging, from the Administration menu, select Messaging Administration > Networked Machines. 2. Click Add a New Networked Machine: <ol style="list-style-type: none"> a. On the Add Networked Machine page, in the Machine Name field, type the Local Machine Name that you recorded from the General Parameters page on the Message Networking system. b. In the Password field, type the LDAP password that you recorded from the General Parameters page on the Message Networking system. c. In the IP Address field, type the IP Address that you recorded from the General Parameters page on the

	<p>Message Networking system.</p> <ol style="list-style-type: none"> d. In the LDAP Port field, enter the port number if different from the default. e. In the Mailbox Number Length field, type the number of digits in the Network Address Length field that you recorded from the General Parameters page on the Message Networking system. f. In the Default Community field, assign the appropriate ID if different from the default 1. g. Set the Updates In and Updates Out fields to yes. h. For the Mailbox Number Ranges fields, enter prefixes if appropriate. In the Starting Mailbox Number field, type all zeros and in the Ending Mailbox Number field, type all 9s to accommodate all combinations, unless you are using point-to-point networking that might conflict with this range. If you are using point-to-point networking without prefixes, enter the appropriate address ranges for the Messaging Networking system. <p>Click the field names or Help on the Web-based administration page to view more information.</p> <ol style="list-style-type: none"> 3. Click Save to add the Message Networking system to the list of networked machines.
	<p>On the Avaya Aura™ Messaging system:</p> <p>Gather the following information about the Avaya Aura™ Messaging system. Use this information when you administer the Avaya Aura™ Messaging system as a remote machine on Message Networking:</p> <ol style="list-style-type: none"> 1. After logging into the Avaya Aura™ Messaging, from the Administration menu, select Messaging Administration > Networked Machines. 2. On the Manage Networked Machines page, select the local machine from the list and click Edit the Selected Networked Machine. 3. On the Edit Networked Machine page, record the following information: <ul style="list-style-type: none"> o Machine Name o Mailbox Number Length o Mailbox Number Ranges o IP Address <p>Note: You also need to obtain the LDAP password for the Avaya Aura™ Messaging machine. The system does not display the Password for security reasons.</p> 4. Verify that the Updates In and Updates Out fields are set to yes.
	<p>On the Message Networking system:</p> <p>Administer the remote machine parameters for the new Avaya Aura™ Messaging remote machine.</p>
	<p>On the Message Networking system:</p> <p>Administer the Dial Plan Mapping for the remote machine, using the Dial</p>

	Plan Mapping requirements you obtained.
	<p>On the Message Networking system:</p> <p>Perform a remote machine connectivity test for SMTP and LDAP. Verify that the connection was successful.</p>
	<p>On the Message Networking system:</p> <p>Add the Avaya Aura™ Messaging system subscribers to the Message Networking system by performing a Demand Remote Update.</p>
	<p>On the Message Networking system:</p> <p>Verify that the Avaya Aura™ Messaging remote machine has been added to the Message Networking system by viewing the Remote Machines List.</p>
	<p>On the Message Networking system:</p> <p>If the Message Networking system has more than 250,000 subscribers, administer a Directory View for the Avaya Aura™ Messaging system to include no more than 250,000 subscribers. Avaya Aura™ Messaging does not accept more than 250,000 subscribers (with or without voice name) during an update.</p>
	<p>On the Avaya Aura™ Messaging system:</p> <p>Add the Messaging Networking subscribers to the Avaya Aura™ Messaging system. See the Avaya Aura™ Messaging Documentation CD for detailed steps on adding remote subscribers to the Avaya Aura™ Messaging version you are using.</p> <p>Add the Messaging Networking subscribers to the Avaya Aura™ Messaging system:</p> <ol style="list-style-type: none"> 1. After logging into the Avaya Aura™ Messaging, from the Administration menu, select Messaging Administration > Request Remote Update . 2. On the Request Remote Update page, select the Message Networking system from the list and click Request Update. <p>Note: You can click Refresh Update Status to view the progress of the update. If all subscribers are not received, you must determine the cause of the failure.</p>
	<p>On the Message Networking system:</p> <p>Update the other remote machines in the Message Networking network for the new Avaya Aura™ Messaging machine's subscribers.</p> <p>Note: Most remote machines are configured for Dynamic updates.</p>
	<p>Send a test message from another messaging system through the Message Networking, using the network address of the Avaya Aura™ Messaging test mailbox that you obtained from the Avaya Aura™ Messaging system administrator. Then log in to the test mailbox on the Avaya Aura™ Messaging system and verify that the test message was delivered.</p>





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Message Networking subscribers



Message Networking subscribers

A Message Networking subscriber is a subscriber on an administered remote machine that has been identified on the Message Networking system. The [average number of supported subscribers](#) and the [subscriber capabilities](#) depend on the remote machine type.

Note: A maximum of 500,000 subscribers (250,000 with voice names) are supported for Message Networking. Enterprise Lists and Enterprise List voice names also count as subscribers on the system.

Message Networking subscribers can be administered in the following ways:

- Using a third-party application through the system's secure [LDAP interface](#).
- [Manual updates through the administration interface](#)
- [Self-registration mailbox](#)
- [Remote updates](#)
- [Bulk subscriber administration](#)

Before administering remote subscribers, you should be aware of differences in subscriber functionality due to use with Message Networking. See [Remote machine considerations](#) for more information.

When a new node is added to the messaging network, Message Networking either pulls the new subscriber information or the new subscriber information is "pushed" to the Message Networking system. Whether information is pulled or pushed depends on the particular nodes involved in the messaging exchange. Subscriber information can be made available to other nodes once it is on the Message Networking system. For more information on Message Networking subscribers, see [Subscriber administration](#).

[Top of page](#)



Connection type	Average subscribers on an S8800 2U server				
	Very heavy usage	Heavy usage	Medium usage	Light usage	Very light usage
Digital					
AUDIX TCP/IP		4,860	19,440	113,400	202,500
Aria TCP/IP	1,620	3,240	12,960	89,100	178,200
Serenade TCP/IP	1,620	3,240	12,960	89,100	178,200
SMTP TCP/IP (VPIM and MIME)	2,025	4,050	16,200	89,100	178,200
Analog					
AMIS or Octel Analog (at 12 port capacity)	320/480	640/960	1,920/2,880	12,800/19,200	25,600/38,400
AMIS or Octel Analog (per group of 4 ports)	80/240	160/480	480/1,440	3,200/9,600	6,400/19,200

The following table lists the average subscribers on a Message Networking system with an S3500 Basic server.

Connection type	Average subscribers on an S3500 Basic				
	Very heavy usage	Heavy usage	Medium usage	Light usage	Very light usage
Digital					
AUDIX TCP/IP	1,000	2,000	8,000	48,000	96,000
Aria TCP/IP	500	1,000	4,000	28,000	56,000
Serenade TCP/IP	500	1,000	4,000	28,000	56,000
SMTP TCP/IP (VPIM and MIME)	1,000	2,000	8,000	46,000	92,000
Analog					
AMIS or Octel Analog (at 12 port capacity)	300	600	1,800	12,000	24,000

AMIS or Octel Analog (per group of 4 ports)	100	200	600	4,000	8,000
---	-----	-----	-----	-------	-------

The following table defines the usage profiles used when calculating the average subscribers for each connection type. The usage levels are defined for each message component type.

Component Type	Average Component Size	Average Number of Messages/Subscriber/Day (in and out)
Voice	(Seconds) Short=30, Medium=60, Long=120	Very light=0.2, Light=0.4, Medium=2.0, Heavy=4.0, Very heavy=8 Use approximately 25% more if Enterprise Lists will be used on a AMIS system in the network.
Fax	(Pages) Short=1, Medium=3, Long=5	Very light=0.1, Light=0.2, Medium=1.0, Heavy=2.0, Very heavy=4.0
Text	(Kbytes) Short=1, Medium=5, Long=10	Very light=2.0, Light=4.0, Medium=10.0, Heavy=20.0, Very heavy=40.0
Binary	(Kbytes) Short=10, Medium=100, Long=200	Very light=2.0, Light=4.0, Medium=10.0, Heavy=20.0, Very heavy=40.0

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Message Networking subscribers](#) > Subscriber capabilities

Subscriber capabilities

The following lists the subscriber capabilities of a Message Networking system:

- The Message Networking system requires a uniform length dial plan (the number of digits used when addressing a message). It consists of a network address of from 3 to 10 digits. A 10-digit network address dial plan is recommended.
- Message Networking supports variable-length addressing, which allows Modular Messaging subscribers to address messages to subscribers on other remote machines using an alternate numbering. See [Administering numeric address mapping](#) for more information.
- A subscriber must be administered on a Message Networking system so that Message Networking can accept messages for delivery.
- Messages sent by digitally networked mailboxes to subscribers on any supported remote machine can be addressed using the number or name of the subscriber, if the subscriber name has been administered or registered.

Note: Data must have been previously downloaded to the remote digital sending machine from the Message Networking system.

- Messages sent to digitally networked mailboxes from subscribers on any type of end node are treated as though they are coming from another digitally networked mailbox. Recipients hear "Message from *voice or extension*" as they usually would when receiving a message from local subscribers.

Note: For VPIM V2 end nodes, this capability depends on the features of the VPIM end node.

- AMIS Analog subscriber messages can optionally contain the "private/priority" designation and voiced name of the sender as part of the actual message being sent.
- Messages delivered to VPIM V2 digital subscribers include the sender's name in the appropriate sender's voice name field in the ADPCM form if the name is stored on the Message Networking system.
- VPIM V2 digital subscriber messages can optionally contain the "private/priority" designation and voiced name of the sender as part of the actual message being sent.

Note: When Aria senders send a mixed private and/or priority message to multiple Serenade or VPIM V2 digital recipients on the same remote machine, the message is marked Priority and/or Private for all recipients, even if only one recipient is marked as such. The sender is not notified that this has happened.

- AMIS Analog and Octel Analog Networking subscribers can be administered through any of the following ways:
 - Message Networking Web- Administration pages
 - Bulk files
 - Sending a message through the Message Networking system (Octel Analog Networking only)
 - Demand Remote Update (Octel Analog Networking only)
 - Sending a message to a predefined subscriber registration mailbox on the Message Networking system
 - Professional Services Organization (PSO)
- Aria Digital and Serenade Digital subscribers can be administered through any of the following ways (refer to Appendix H, Directory Population, in Message Networking Administration for further information about how and when subscribers are added to the Message Networking system):

- NameSend from Aria or Serenade Digital.
 - Note:** For existing subscribers who were migrated from an Aspen system to Aria Release 2.05 or later, NameSend does not work until each subscriber rerecords a spoken name on the Aria.
- For Aria, Demand Remote Update from the Message Networking system is supported as follows:
 - Can be done by all extensions or an extension range.
 - Takes an average of 2 seconds per subscriber.
 - Is less efficient than Aria NameSend.
- Aria/Serenade Digital automatically informs the Message Networking system when a new subscriber is added; this is similar to AUDIX directory updates.
- Duplicate names from the same Serenade system have **Node #D#** appended to the name to make it unique.
- Except for Serenade Octel Analog and Serenade Digital, Message Networking does not support multiple mailbox ID lengths within the same remote machine (message server). Each remote machine can have a different mailbox ID length, but the length of mailbox IDs cannot vary within a given remote machine. For Serenade Octel Analog and Serenade Digital remote machines, the Message Networking system can be administered to map multiple mailbox ID lengths to the uniform Network Address length.
- VPIM V2 and SMTP/MIME (that do not use LDAP-based updates) subscribers can be administered in any of the following ways:
 - Message Networking Web- Administration pages
 - Bulk files
 - Sending a message through the Message Networking system
 - Self-registration
- For subscribers residing on AUDIX Digital remote machines, a *delivered* status means the message was successfully delivered to the Message Networking system. This message can be returned to the sending subscriber if the Message Networking system cannot successfully deliver the message to the receiving subscriber for some reason.
- A *scheduled message* status for AUDIX indicates that delivery has not been successfully completed, nor has it failed yet.
- Senders receive notification of failed messages in two ways, including:
 - An error message indicating each mailbox that failed to receive the sent message. This can be an optional Priority message.
 - A copy of the failed original message from the Failed Message Delivery Manager.
- For AUDIX, failed message IDs can be viewed using INTUITY Message Manager.
- Notification of failure to deliver a message component because the recipient is not enabled to receive a component type (voice, fax, text, or binary) is the same as on the INTUITY AUDIX Release 4 system. The component that could not be delivered is stripped, and the following is prefixed to the original message: "One or more components could not be delivered, please contact the sender <pause><voice message>."
- *Accessed* status indicates that the subscriber has received and accessed a message for both the Message Networking and INTUITY AUDIX systems.
- For AUDIX, the machine name of the receiving machine in INTUITY Message Manager is that of the Message Networking system delivering the message.
- The ASCII name for remote subscribers contains a suffix of from two to eight characters at the end of the name field, indicating the Message Networking node ID for the remote machine on which that subscriber resides.





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Enterprise Lists overview



Enterprise Lists overview

Message Networking supports the creation and administration of Enterprise Lists, which are enterprise-wide mailing lists for subscribers that reside on a Message Networking system. Each Enterprise List represents a specific group of potential recipients for enterprise distribution messages. Enterprise Lists can be used to send messages to literally hundreds of thousands of subscribers across the enterprise, and to members of the different messaging systems that Message Networking supports.

Note: Enterprise Lists are supported on S3500-H and S8800 2U servers.

This topic provides the following information about Enterprise Lists:

- [How Enterprise Lists work](#)
- [Enterprise List members](#)
- [Number of support Enterprise Lists](#)
- [Maximum number of recipients in an Enterprise List](#)
- [Usage considerations](#)

See [Administering Enterprise Lists](#) for information on list administration.

Caution: It is important that you understand list creation before using the Enterprise List feature. If an error is made, a message could be sent in error to hundreds or thousands of subscribers within your network.

How Enterprise Lists work

When an Enterprise List is created, members are added to the list by one of several different criteria that are then stored under that list ID. When a message is sent to the list, the system finds list members based on the stored membership criteria, checks appropriate permissions for using the list, and expands the list so that the message can be delivered to each recipient. Because the Enterprise List application uses a virtual subscriber as the actual list ID, anyone who is networked to the application and who has permission to use the list can access it from any remote machine. In addition, those permitted to send messages using Enterprise Lists can reference lists by:

- Number (including network address or numeric address)
- Alphabetic Name (ASCII name)
- Speech Voice Name (by providing the alphabetic name)

Note: The addressing method used depends on the individual messaging system that the sender uses and the user interface of that system. User interfaces such as Web Messenger or other IMAP 4 clients might also be used to address Enterprise List messages.

If the [moderator](#) role for an Enterprise List is active, every message sent to the list is first sent to the moderator. The moderator is responsible for approving or rejecting the full delivery of each message. After the moderator approves a message, the system delivers it to all members of the list.

Note: A moderator must be an SMTP/MIME type sender.

Enterprise List members

Valid subscribers of a Message Networking system and other Enterprise Lists can be selected as Enterprise List members. Message Networking supports up to twenty levels of embedded Enterprise Lists. An embedded Enterprise List is an Enterprise List that contains another Enterprise List.

System administrators are responsible for managing various permissions for Enterprise List members, including permission to create and update lists. However, these permissions are only available to system subscribers who use a lightweight directory access protocol (LDAP) client. Enterprise List administrators can also choose whether a list is or is not subscription-based. A subscription-based list allows LDAP clients who are not currently members to request that they be added to the list. If a list is not subscription-based, its members are determined by the list administrator.

Note: Certain Enterprise List features might not be accessible to specific sender or recipient types depending on the configuration of external software clients accessing the Enterprise List database. Most general message sending and receiving capabilities are supported for all subscriber types.

Number of supported Enterprise Lists

The number of subscribers plus the number of Enterprise Lists plus the number of Voice Name Mailboxes cannot exceed 500,000, with the following conditions:

- The total number of voice names in the entire system cannot exceed 250,000.
- Each individual recipient is counted only once as a subscriber, regardless of how many Enterprise Lists to which that recipient belongs.
- Each Enterprise List counts as a subscriber.
- Each voice name mailbox, which is required for Enterprise Lists with voice names, is counted as a subscriber with a voice name.

For example, an enterprise having 100,000 recipients could have up to 75,000 Enterprise Lists with Voice Name Mailboxes in the system, (assuming all subscribers and Enterprise Lists have voice names):

Maximum number of subscribers Message Networking supports:	250,000
Minus individual recipients in the enterprise:	100,000
Equals maximum number of Enterprise Lists and Voice Name Mailboxes in the system:	150,000

Maximum number of recipients in an Enterprise List

Based on the example above, the maximum number of recipients is simply the maximum number of subscribers in the network.

The number of total subscribers that Message Networking supports (500,000, or 250,000 with voice names) minus the number of Enterprise Lists and Voice Name Mailboxes equals the total number of possible recipients per list. An individual recipient is counted only once as a subscriber, regardless of how many Enterprise Lists to which that recipient belongs.

For example, an enterprise having 25,000 Voice Name Mailboxes and 75,000 enterprise lists could have up to 400,000 recipients per list, as shown in the following table:

Maximum number of subscribers Message Networking supports:	500,000
Minus Enterprise Lists in the system:	75,000
Minus Voice Name Mailboxes in the system:	25,000
Equals maximum number of individual recipients per list:	400,000

Usage considerations

The Enterprise List feature is a powerful application that can be used to send a message to literally hundreds of thousands of subscribers across the enterprise, however it is important to note the following considerations

when using Enterprise Lists.

1. Enterprise Lists are lists and not a broadcast feature. The term broadcast implies that the sender has the option to invoke Message Waiting Indication (MWI). Examples of MWI include lighting the light on a telephone set and outcalling. Enterprise Lists invoke MWI to notify the recipient of message receipt. For some networks, the effects of MWI should be strongly considered when using these lists. Invoking MWI for a large number of subscribers on an end node can consume significant system and/or network resources. However, in many existing networks, messages are sent to every subscriber in the Enterprise without any issues with MWI.

Workarounds are available for the following messaging systems if MWI is not desired for a receiving system:

- Intuity AUDIX - an Enterprise List can be built referencing one subscriber per Intuity system that has local broadcast permission on that Intuity system. Upon receiving the Enterprise List message, that person can forward the message to the local Intuity broadcast mailbox with MWI turned off.
 - Aria - an Enterprise List can be built referencing the bulletin broadcast mailbox on each Aria system. Sending messages in this fashion will not invoke MWI when sent to all of the Aria recipients. These recipients must have the bulletin broadcast class of service (COS).
 - Serenade - System Distribution Lists (SDL) on Serenade have an MWI option. An Enterprise List can be built referencing a Serenade SDL with MWI turned off.
 - Modular Messaging- Using the Modular Messaging/Avaya Enhanced List Application (ELA) feature, a system broadcast ELA can be built without MWI. A Message Networking Enterprise List can reference this Broadcast ELA, sending a message to all Modular Messaging recipients not invoking MWI.
2. In large networks that include more than one Message Networking system, avoid defining a list with a large range on system A that includes subscribers whose home system is system B. For example, if range 5550000-5559999 is on system A and range 6660000-6669999 is on system B, then break these down into two separate lists on each respective system. One list id can be created to reference both lists so that the separate lists are transparent to the sender. This will distribute system processing and help performance.
 3. The time required to deliver messages to their entire enterprise depends on the following factors:
 - The throughput of the WAN/LAN.
 - The type and number of TCP/IP endpoints (INTUITY AUDIX, Octel 250/350, Octel 200/300 servers) as transcoding takes more time.
 - The number/type of endpoints and the distribution of the subscribers.
 - Number of any other non-TCP/IP endpoints (Octel Analog, AMIS).
 - Number of Message Networking systems (distribution).
 - Other message traffic load occurring at the same time (both on Message Networking and the endpoint).
 - Other performance-impacting activities (e.g. running of reports, etc.) both on Message Networking and the endpoint.
 - Number and type of ports configured on each system/endpoint.

The following example can be used for comparison. A customer sends a message to all 40,000 subscribers in an INTUITY AUDIX (that is, there is no digital transcoding) network during non-prime time. Network Address Ranges are used in the Enterprise List feature. In this example, the entire delivery process takes 3.5 hours.

4. Message Networking supports hybrid network configurations in which there is a mix of point-to-point and Message Networking message server connections. In configurations such as this, however, there exists the possibility for double remote name entries. When this occurs, two remote subscriber directory entries can be stored on the local message server for one system subscriber: one for the point-to-point path and another for the Message Networking path. In this case, senders using the dial-by-name feature can get back two responses for the same person (for example, "Press 1 for John Smith, Press 2 for John Smith").

Users can prevent this double name entry by [administering directory views](#) on the Message Networking system to exclude remote machines to which they are connected point-to-point.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Administration](#) > [Administering Enterprise Lists](#) > Enterprise List moderator overview



Enterprise List moderator overview

This topic provides general information about the role of the Enterprise List moderator and provides a link to more detailed instructions, which will be useful to those occupying the role of moderator.

An Enterprise List moderator, which you can activate during the creation or modification of a list, acts as a gatekeeper for all messages sent to a list. Each message is sent to the moderator first, along with a request for approval. The message cannot be distributed to members of the list without the moderator's approval.

The moderator must respond to the request for approval before the status message expiration time occurs. This value is set on the Message Networking [General Parameters](#) page. If the moderator does not respond within this time, the message is deleted and is not sent to any recipients. The default value for the status message expiration time is seven days.

Note: The moderator role is only supported for SMTP/MIME systems. A moderator must be a valid subscriber on an SMTP remote machine, such as Modular Messaging.

Requests for approval that are sent to the moderator include the contents of the message and the following message information:

- List number
- Name of the list to which the message is being sent
- Originator's name and network address

See [Enterprise List moderator instructions](#) for detailed moderator instructions, including reply options and ways of communicating directly with the Message Networking system.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Simple Network Management Protocol overview



Simple Network Management Protocol overview

The Simple Network Management Protocol (SNMP), a current working standard of the TCP/IP protocol suite, is used to transfer network management information among various elements of a network, regardless of their underlying architecture.

SNMP can be used with Message Networking to perform the following tasks:

- As a manager, a network management station (NMS) can perform [queries of system status information](#) from Message Networking and receives notifications. SNMP is read-only in the Message Networking system, meaning that an NMS can query a Message Networking system for information, but cannot change that information.
- As an agent, the Message Networking system responds to configuration requests and sends [alarm and resolution event notifications](#) to specified NMSs through SNMP.

Most SNMP information is accessed synchronously and on demand using get and set requests. In essence, SNMP uses a client/server relationship in which the NMS is the client and Message Networking is the server. Message Networking can communicate with one or more NMS asynchronously for alarm notification.

SNMP information is organized in a hierarchical tree. A [Management Information Base \(MIB\)](#) defines the structure of information in the hierarchical tree. Message Networking supports the standard Management Information Base (MIB-II) definition, as well as private Avaya MIBs that supports SNMP queries and alarm notification. See [Simple Network Management Protocol MIBs](#) for information on the MIBs used by Message Networking for SNMP.

Message Networking supports SNMP versions 1, 2c, and 3. Any monitoring software that is SNMP v1, SNMP v2c, or SNMP v3 compliant, including Avaya AIM software, can communicate with Message Networking.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > SNMP system queries overview



SNMP system queries overview

An SNMP network management station (NMS) can perform queries of system status information from Message Networking. SNMP is read-only in the Message Networking system, meaning that an NMS can query a Message Networking system for information, but cannot change that information.

You can request the following types of information about a Message Networking system via SNMP queries:

System information:

- Version installed
- Module uptime
- Active alarms (major, minor, and warning)

Network information:

- Number of machines administered on the Message Networking system
- Number of messages waiting to be transmitted
- Active network connections:
 - Digital (TCP/IP, SMTP, VPIM)
 - Analog (AMIS, Octel Analog Networking)

The method used to authenticate queries depends on the version of SNMP running on the NMS making the request:

- For versions 1 and 2c, [community](#) strings are required to secure access.
- For version 3, [users](#) (views) are required to secure access to SNMP information.

See [Administering SNMP](#) for information on the steps you must complete to administer SNMP queries on the Message Networking system.



[Getting Started](#)[Administration](#)[Installation](#)[Maintenance](#)[Reference](#)

[Home](#) > [Message Networking concepts and features](#) > [Simple Network Management Protocol overview](#) > Simple Network Management Protocol MIBs



Simple Network Management Protocol MIBs

In SNMP, the Structure of Management Information (SMI) is the standard that defines the rules for identifying managed objects. SMI also defines the:

- Syntax for sending and receiving information.
- Means for organizing information into logical groups.
- Naming mechanisms, known as object identifiers, that identify managed elements.

SMI requires all managed elements in the SNMP environment to be arranged in a hierarchical structure known as a Management Information Base (MIB), which is a special kind of database for network management information.

The SMI structural design that MIBs must follow is sometimes referred to as a tree. Branches of this tree represent the logical grouping of information objects. Each end node, or leaf, represents a piece of information to be managed and has a unique identifier to define its location on the MIB tree. This identifier consists of a string of integers separated by periods. Alternately, in text descriptions, the identifier can consist of a series of text strings separated by periods.

Starting at the root of the tree, the tree branches out until each object has been placed and defined with both an integer string and a text string.

Message Networking uses the following MIBs:

- The standard Management Information Base (MIB)-II definition.
- Avaya-provided MIBs:
 - [mnMib.txt](#): This MIB includes information specific to the Message Networking application.
 - [avaya_snmp_mib.txt](#): This MIB includes information related to alarm notification to a primary NMS.
 - [avaya_oam_mib.txt](#): This MIB includes information related to alarm notification to secondary NMSs.

See [Transferring Avaya MIBs to SNMP network management stations](#) for information on transferring the necessary Avaya MIBs to each NMS that requires a copy.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Alarm notification overview



Alarm notification overview

You can administer Message Networking to perform alarm notification through SNMP or SAL (via SAL Gateway) to specified NMSs (Network Management Stations).

Types of Message Networking alarm notifications include:

- Major alarm raised
- Minor alarm raised
- Warning alarm raised
- Alarm resolved

Message Networking system can be configured to send alarm notifications and events to a service organization using SPIRIT or SAL. Message Networking can also use SNMP or SAL (via SAL Gateway) to send these notifications to a customer NMS. All Message Networking systems are installed with SPIRIT, which provides remote serviceability using IP access. SPIRIT replaces the older modem-access agents, including Avaya Serviceability Agent.

You can administer NMSs for alarm notification through SNMP or SAL. You can administer NMS from the Message Networking Web interface:

- **Configure Alarms:** Under **Alarming**, click **Alarm Configuration**. The system displays the **Configure Alarms** page. On this page set the **Alarm Origination** to one of the following types of alarm notification:
 - INACTIVE
 - MODEM DIALOUT
 - SNMP
 - INTERNET
 - SAL

If the alarm notification is set to MODEM DIALOUT, you can also specify network management stations (NMSs) on the **Administer SNMP Trap Destinations** page.

- **Administer SNMP Trap Destinations:** Under **Alarming**, click **SNMP Trap Destinations**. The system displays the **Administer SNMP Trap Destinations** page. Administer NMSs to monitor system alarms. If the alarm notification is set to SAL, SAL Destinations are administered on the SAL Destinations page. Network Management stations are administered on the SAL Gateway. You can set the following NMSs:
 - The OAM NMS is customer provided NMS. **OAM** NMS is used to monitor the system alarms, but not to acknowledge alarm notification. OAM receive more alarms than INADS destination.
 - The INADS NMS is Avaya or Avaya Business Partner provided NMS. **INAD** NMS is used to send alarms for Avaya product deployment to the Avaya Technical Service Center or to products that act like the Avaya Technical Service Center.

See [Administering SNMP](#) for information on the steps you must complete to administer NMSs for alarms on the Message Networking system.

Administering SAL Destination

To administer SAL destination, under **Alarming**, click **SAL Destination**. The system displays the **Add New**

SAL Destination page. Administer SAL Destination to monitor system alarms. INADS and OAM NMSs are administered on the SAL Gateway.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Concepts and features](#) > Message Networking language support



Message Networking language support

Message Networking supports the ability to specify the language in which system announcements are voiced. Announcements are of two types:

- Announcements sent back to the originator of the message
- Announcements sent/attached to the recipient's message

Installing or updating languages on Message Networking

The languages that Message Networking supports are provided in the Avaya Message Networking Application Software media. US English is always installed on the system. See [Installing switch connection software and language packages](#) for detailed steps for installing and updating languages. The list of languages supported for use with Message Networking is provided on the Avaya support Web site. Go to <http://www.avaya.com/support> and navigate to the Message Networking page.

Deleting languages from Message Networking

You can delete individual languages from the Message Networking system if necessary. For detailed information on deleting languages from the Message Networking system, see [Removing software packages](#).

Note: Do not remove the US English language software package from the system as it is the default language that is used when a subscriber's preferred language is unavailable.

Assigning languages to remote machines and subscribers

Each remote machine defined on the Avaya Message Networking system has a default language, which you specify in the Default Language field when you [administer a remote machine](#). Initially, all subscribers administered on a remote machine are assigned the remote machine default language as their preferred language. However, you can modify an individual subscriber's language, either by changing the **Language ID** field on the [Subscriber Administration page](#) or through [bulk administration by file](#) (except Avaya Modular Messaging, Avaya Aura™ Messaging and remote Avaya Message Networking systems, which use LDAP-based directory updates).

The language id is used and displayed in the following locations in the Message Networking application:

1. The **Default Language** field on the [Remote Machine Parameters Administration](#) page.
2. When subscribers are [added or modified in bulk using FTP files](#).
3. The **Lang ID** field in the [Subscriber List reports](#) (by Name, by Network Address, by Mailbox ID, and by Remote Machine Name).
4. The **Language ID** field on the [Subscriber Parameter Administration page](#).
5. The **Language ID** field on the [Subscriber Parameter Display page](#).

Determining the language used to generate announcements

When determining the language in which to generate an announcement, Message Networking applies the following criteria, in order of preference:

1. If the subscriber's assigned Language ID is available on the Message Networking system, that language is used.

2. If the assigned Language ID is not available, but a variant of the language is available, the language variant is used. For example, if fr-CA is the subscriber's assigned Language ID and fr-FR is installed but fr-CA is not, then fr-FR is used. If more than one variant is available, the variant that comes first alphabetically is used.
3. If neither the Language ID nor a variant is available, en-US (US English), which is always available, is used.

General considerations

Note the following considerations associated with Message Networking language support:

- The following are available in US English only:
 - The voice names associated with system mailboxes.
 - The existing system mailboxes have a voiced name of "The Network." The system mailboxes (reserved in number from 0000000000-0000000010) are those mailboxes that Avaya Message Networking-generated messages originate from (for example, failure notification).
 - Full language support is available only in a multi-hub environment scenario where all systems are Avaya Message Networking 2.0 or later versions.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Bridging feature overview



Bridging feature overview

Message Networking supports a bridging feature in which Message Networking is used to transmit messages to or from remote machines designated as bridged machines. With this feature, Message Networking no longer acts as a hub for all message activity between remote machines in the network. Instead, Message Networking only allows messages to pass between two remote machines when one of the remote machines is designated as a bridged remote machine. Any attempts to send messages directly between nonbridged remote machines fail.

This feature supports both the [bridge and hybrid network configurations](#) supported by Message Networking. If you want to use Message Networking in a hub-and-spoke network configuration, you cannot use the bridging feature.

The Number of Bridged Nodes parameter on the [Customer Options page](#) determines whether the Message Networking system is being used in a hub-and-spoke or bridge configuration:

- When the Number of Bridged Nodes is set to 500 (the maximum), the system is being used in a hub-and-spoke configuration. This parameter is always set to 500 for Message Networking systems running on the S3500-H and S8800 2U servers.
- When the Number of Bridged Nodes is set to a number below 500, this parameter specifies the number of remote machines that can be designated as bridged systems. When bridging is used, a parameter on the Remote Machine Administration page allows you to designate a remote machine as a bridged machine. The number of remote machines that you designate as bridged machines cannot exceed the Number of Bridged Nodes specified on the Customer Options page.

Note: If the number of systems administered as bridged machines equals the Number of Bridged Nodes on the Customer Options page, you must **not** modify the Number of Bridged Nodes parameter to reduce the number of bridged nodes. If you do, the system removes the bridging from the first system you administered as a bridged machine.

For more information, see [Sample Message Networking Bridged Networks](#).

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

Getting Started

Administration

Installation

Maintenance

Reference

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > [Bridging feature overview](#) > Sample Message Networking Bridged Networks



Sample Message Networking Bridged Networks

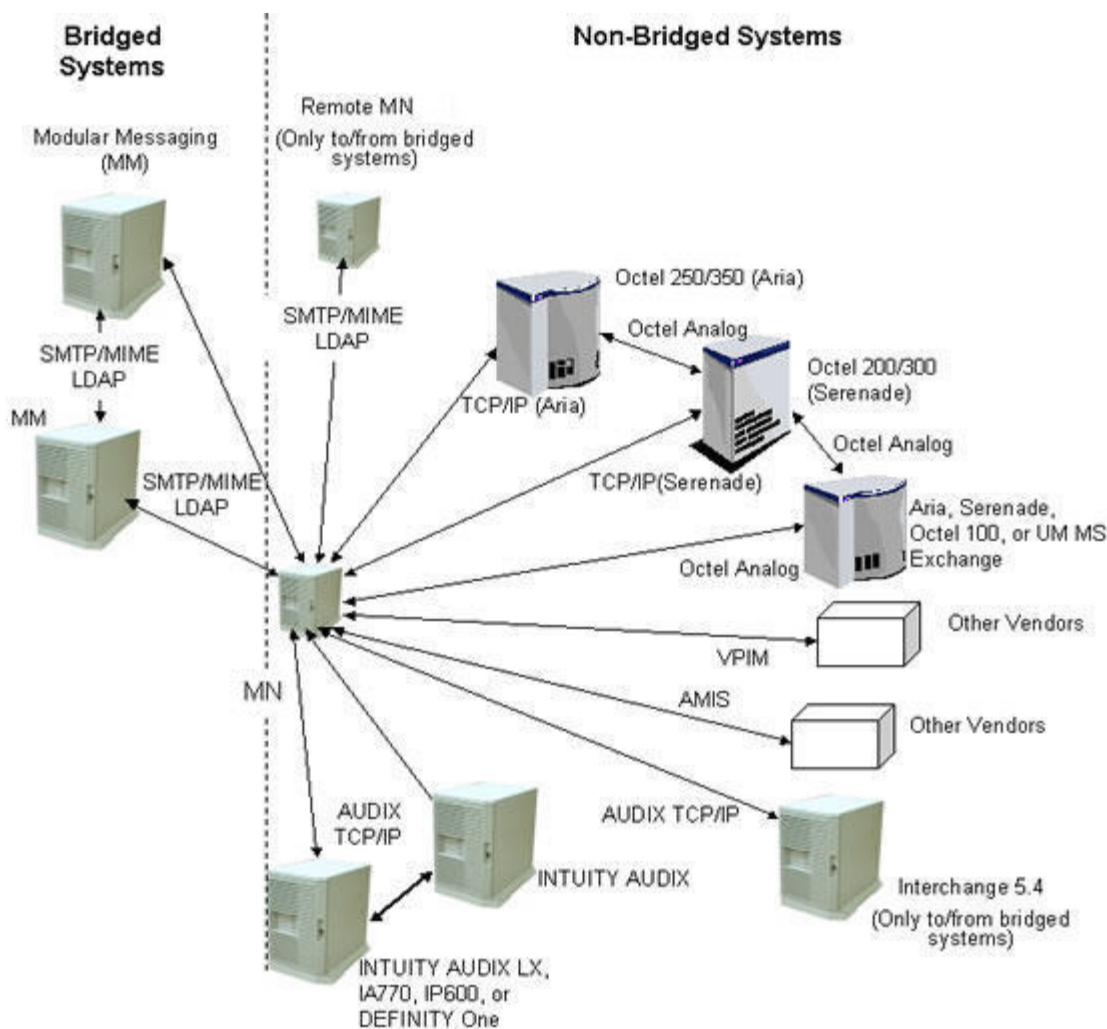
Message Networking supports a bridging feature in which Message Networking is used to transmit messages to or from remote machines designated as bridged machines. With this feature, Message Networking no longer acts as a hub for all message activity between remote machines in the network. Instead, Message Networking only allows messages to pass between two remote machines when one of the remote machines is designated as a bridged remote machine. Any attempts to send messages directly between nonbridged remote machines fail.

This document provides two sample Message Networking bridged networks:

- A system in which Modular Messaging systems are bridged to a network.
- A system in which a Unified Messenger system is bridged to a network.

Sample 1: Bridged Modular Messaging system

The following figure depicts a sample Message Networking bridged network in which two Modular Messaging systems are administered as bridged systems. The systems on the left side of the dotted line (the two MM systems are designated as bridged systems. The systems on the right side of the dotted line are remote machines in the network that are not designated as bridged systems. The straight lines indicate the message paths that are supported.

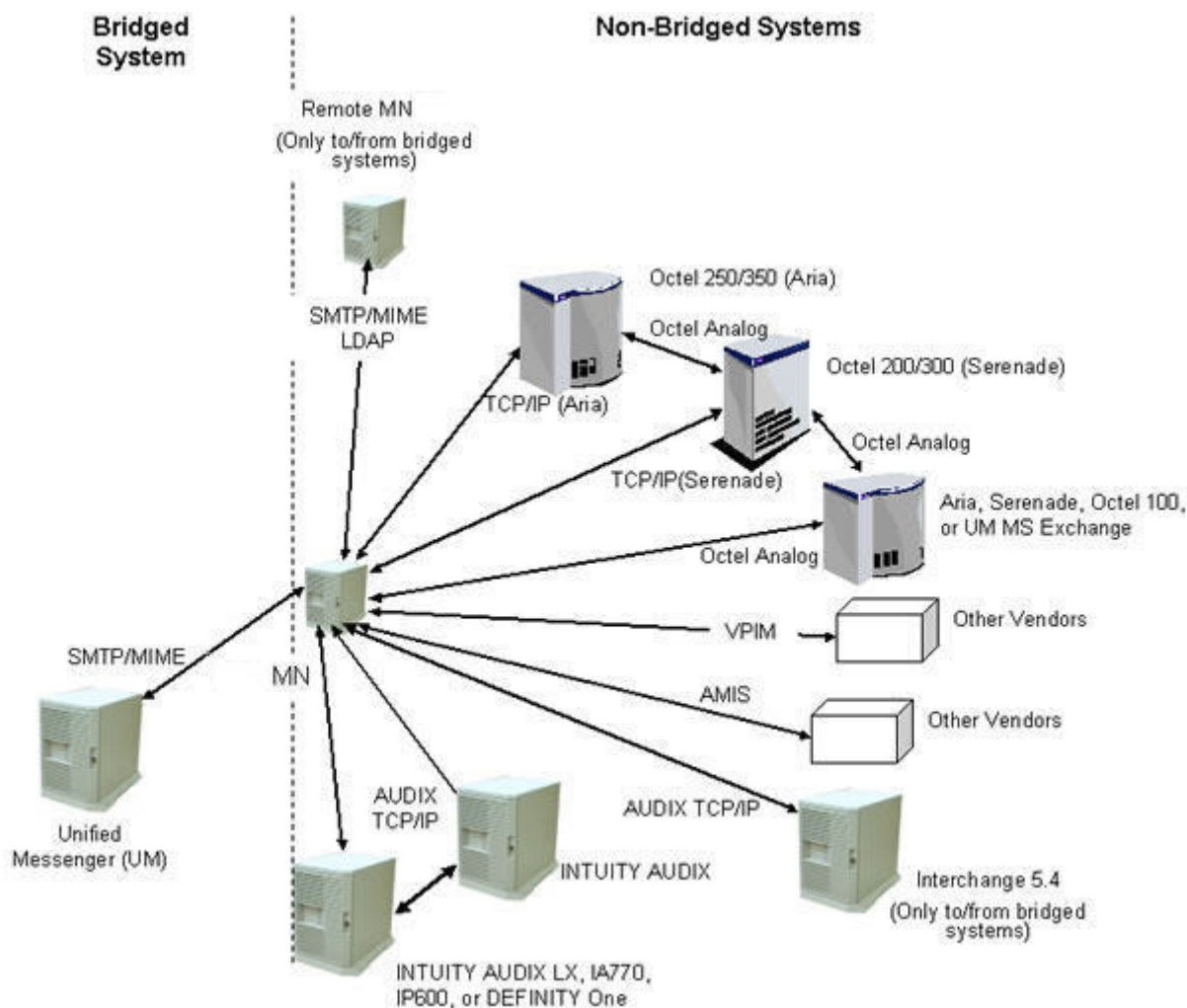


In this configuration:

- A message sent from one of the Modular Messaging system to the INTUITY AUDIX through Message Networking is delivered because the Modular Messaging system is designated as a bridge.
- A message sent from the INTUITY AUDIX to the Octel 250/350 through the Message Networking bridge fails with a “sending restrictions” error code because neither the INTUITY AUDIX nor the Octel 250/350 systems is a bridged system.
- A message sent directly from the Octel 200/300 to the Octel 100 is delivered because the message is not sent through the Message Networking system and those system can communicate directly through Octel Analog.

Sample 2: Bridged Unified Messenger system

The following figure depicts a sample Message Networking bridged network in which one Unified Messenger system is administered as a bridged system. The system on the left side of the dotted line (the UM system) is designated as a bridged system. The systems on the right side of the dotted line are remote machines in the network that are not designated as bridged systems. The straight lines indicate the message paths that are supported.



In this configuration:

- A message sent from the UM to the Octel 250 through Message Networking is delivered because the UM system is designated as a bridge.
- A message sent from the INTUITY LX to the Serenade 300 through the Message Networking bridge fails with a “sending restrictions” error code because neither the INTUITY LX nor the Serenade 300 system is a bridged system.
- A message sent directly from the Octel 200/300 to the Octel 100 is delivered because the message is not sent through the Message Networking system and those system can communicate directly through Octel Analog.





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#) [Administration](#) [Installation](#) [Maintenance](#) [Reference](#)

[Home](#) > [Administration](#) > [Administering remote machine](#) > Overview of MultiSite for Message Networking



Overview of MultiSite for Message Networking

Customers can connect a Modular Messaging MultiSite/ MSS systems with Message Networking just like they connect other messaging systems. The MultiSite feature is supported on Modular Messaging/ MSS from Release 5.0 and later versions, and on the Avaya Aura™ Messaging system. This topic provides an overview of the MultiSite feature in Message Networking for a MultiSite enabled Modular Messaging remote machine.

What is MultiSite?

MultiSite allows you to use a single Modular Messaging system to serve subscribers at multiple locations. With MultiSite, Message Application Servers (MASs) in a single Voice Mail Domain (VMD) communicate with multiple PBXs possibly with different dial plans, in different locations. Modular Messaging MultiSite/ Message Storage Server (MSS) systems support mailbox numbers of lengths up to 50 digits.

Networking with Message Networking

Message Networking voice networks have network addresses with a fixed length of up to 10 digits. To join such a network a MultiSite enabled Modular Messaging systems can have mailbox numbers of variable lengths.

Mailbox ID Length

Message Networking Release 5.2 allows the customers to connect an Avaya Modular Messaging MultiSite/ MSS systems as a remote machine. Message Networking supports mailbox numbers from 3 digits to 30 digits for a MultiSite enabled Modular Messaging systems. In practice, the mailbox and extension numbers of a Modular Messaging MultiSite systems are unlikely to be longer than 15-digits, the maximum length of an E.164 phone number. Message Networking also allows you to define up to 27 different mailbox number lengths per Modular Messaging MultiSite/MSS remote machines.

Dial plan Mapping

Message Networking uses a uniform, single-length dial plan for its network. Generally, the network address length is 10 digits. The network address dial plan mapping is more flexible for a Modular Messaging MultiSite/ MSS systems. Following are the possible cases:

- Mailbox numbers that are longer than the system network address length are shortened as appropriate.
- Mailbox numbers that are shorter than the system network address length are lengthened as appropriate.
- Mailbox numbers that are already formatted appropriately are used as the network address without further manipulation.

Some examples of network address dial mappings to convert E.164-style mailbox numbers of varying lengths to a 10-digit network address

Example mailbox number	Map From	Map To	Example network address

13035381234	1		3035381234
Remove the 1 from the start of the mailbox number to leave a 10-digit network address.			
441895454567	44189545	986555	9865554567
Replace the UK country and area codes with a fake US area code to give a 10-digit network address.			
670	670	987670	9876701987
Insert a fake US area code before the complete Tokelau number to give a 10-digit network address.			

Mailbox ID to network address translation

The following table shows the translation of addresses when a subscriber on a Modular Messaging MultiSite systems compose a message to the subscriber on an Octel system, and the message is delivered through Message Networking. The translation happens in the following sequence:

Step number	Translation step	From address	To address
1	Subscriber on Modular Messaging MultiSite systems sends a message	13035381234 (Modular Messaging subscriber's full mailbox number)	9089531234 (Remote recipient's Message Networking network address)
2	Message Networking translates address and delivers the message	13035381234 ----> 3035381234 (Strips the leading 1 from the mailbox number.)	9089531234 ---> 1234 (Looks up for 9089531234 in network address directory to find details of the destination node, and the mailbox number within that node.)
3	Message arrives in Octel mailbox	3035381234 (Message Networking network address)	1234 (Octel subscriber's mailbox number)

The following table shows the translation of addresses when the Octel subscriber replies to the sender of that message. The translation happens in the following sequence:

Step number	Translation step	From address	To address
1	Octel subscriber replies to Modular Messaging MultiSite systems subscriber's message	1234 (Octel subscriber's mailbox number)	3035381234 (Message Networking network address)
2	Message Networking translates address and delivers the message	1234 ---> 9089531234 (Inserts 908953 at the start of the address.)	3035381234 ---> 13035381234 (Looks up for 3035381234 in network address directory to find details of the destination node, and the mailbox number within that node.)
3	Message arrives in Modular Messaging MultiSite systems subscriber's mailbox	39089531234 (Message Networking network address)	13035381234 (Modular Messaging full mailbox number)

Note: Modular Messaging MultiSite mailbox numbers are stored by Message Networking in their native form so that network addresses can be converted back into mailbox numbers.

Telephone number administration

When you configure a Message Networking remote machine on the MSS, ensure that the imported telephone numbers are in canonical format by configuring telephone number mappings. After you have configured the telephone number mappings, the system automatically appends a “+” before the telephone number. When a MultiSite enabled Modular Messaging systems are configured as a remote machine on a Message Networking system, or on another Modular Messaging systems, the MultiSite enabled Modular Messaging systems remove the “+” from the beginning of the subscribers’ telephone numbers to avoid problems on the other systems.

Note: Canonical phone numbers follow the international standard (E.164) which allows any publically-accessible phone number to be specified using a standard notation, consisting of an initial + followed only by digits. A code representing the country in which the phone is located comes immediately after the "+". The format used for the rest of the number is country-dependent, but usually the whole number can be broken up like this:

+ CountryCode AreaCode SubscriberNumber

For more information on MultiSite concepts, see Modular Messaging MultiSite Release 5.0 guide on the Avaya support site.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Back](#) | [Fwd](#) | [Close](#)

Getting Started **Administration** **Installation** **Maintenance** **Reference**

[Home](#) > [Administration](#) > [Administering remote machine](#) > Overview of Avaya Aura™ Messaging for Message Networking

Overview of Avaya Aura™ Messaging for Message Networking

Customers can connect the Avaya Aura™ Messaging systems with Message Networking just like they connect other messaging systems. This topic provides an overview of the Avaya Aura™ Messaging and Message Networking

What is Avaya Aura™ Messaging?

Avaya Aura™ Messaging, also referred as Messaging, is the next generation messaging product from Avaya. Messaging is designed for enterprises with complex data and telephony environments. Messaging is flexible, scalable, resilient, and easy to deploy on standard Linux based servers.

Networking with Message Networking

Message Networking voice networks have network addresses with a fixed length of up to 10 digits. To join such a network a Avaya Aura™ Messaging systems can have mailbox numbers of variable lengths.

Mailbox ID Length

Message Networking Release 5.2 allows the customers to connect an Avaya Aura™ Messaging system as a remote machine. Message Networking supports mailbox numbers from 3 digits to 30 digits for Avaya Aura™ Messaging system. In practice, the mailbox and extension numbers of Avaya Aura™ Messaging systems are unlikely to be longer than 15-digits, the maximum length of an E.164 phone number. Message Networking also allows you to define up to 27 different mailbox number lengths perAvaya Aura™ Messaging remote machines.

Dial plan Mapping

Message Networking uses a uniform, single-length dial plan for its network. Generally, the network address length is 10 digits. The network address dial plan mapping is more flexible for a Avaya Aura™ Messaging system. Following are the possible cases:

- Mailbox numbers that are longer than the system network address length are shortened as appropriate.
- Mailbox numbers that are shorter than the system network address length are lengthened as appropriate.
- Mailbox numbers that are already formatted appropriately are used as the network address without further manipulation.

Some examples of network address dial mappings to convert E.164-style mailbox numbers of varying lengths to a 10-digit network address

Example mailbox number	Map From	Map To	Example network address
13035381234	1		3035381234
Remove the 1 from the start of the mailbox number to leave a 10-digit network address.			
441895454567	44189545	986555	9865554567

Replace the UK country and area codes with a fake US area code to give a 10-digit network address.			
670	670	987670	9876701987
Insert a fake US area code before the complete Tokelau number to give a 10-digit network address.			

Mailbox ID to network address translation

The following table shows the translation of addresses when a subscriber on a Avaya Aura™ Messaging system compose a message to the subscriber on an Octel system, and the message is delivered through Message Networking. The translation happens in the following sequence:

Step number	Translation step	From address	To address
1	Subscriber on Avaya Aura™ Messaging systems sends a message	13035381234 (Avaya Aura™ Messaging subscriber 's full mailbox number)	9089531234 (Remote recipient's Message Networking network address)
2	Message Networking translates address and delivers the message	13035381234 ----> 3035381234 (Strips the leading 1 from the mailbox number.)	9089531234 ---> 1234 (Looks up for 9089531234 in network address directory to find details of the destination node, and the mailbox number within that node.)
3	Message arrives in Octel mailbox	3035381234 (Message Networking network address)	1234 (Octel subscriber's mailbox number)

The following table shows the translation of addresses when the Octel subscriber replies to the sender of that message. The translation happens in the following sequence:

Step number	Translation step	From address	To address
1	Octel subscriber replies to Avaya Aura™ Messaging system subscriber's message	1234 (Octel subscriber's mailbox number)	3035381234 (Message Networking network address)
2	Message Networking translates address and delivers the message	1234 ---> 9089531234 (Inserts 908953 at the start of the address.)	3035381234 ---> 13035381234 (Looks up for 3035381234 in network address directory to find details of the destination node, and the mailbox number within that node.)
3	Message arrives in Avaya Aura™ Messaging system subscriber's mailbox	39089531234 (Message Networking network address)	13035381234 (Avaya Aura™ Messaging full mailbox number)

Note: Avaya Aura™ Messaging mailbox numbers are stored by Message Networking in their native form so that network addresses can be converted back into mailbox numbers.





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Message Networking concepts and features](#) > LDAP overview



LDAP overview

The Lightweight Directory Access Protocol (LDAP) is a standards-based protocol for accessing database records that is specifically suited for accessing directory information. This topic provides information on the LDAP interface supported by Message Networking.

LDAP is used in Message Networking as follows:

- Subscriber directory updates between Message Networking systems.
- Subscriber directory updates between Message Networking and Modular Messaging systems.
- Subscriber directory updates between Message Networking and Avaya Aura™ Messaging systems.
- Support for an LDAP interface that you can access through an LDAP client to perform queries of system data and to perform system administration.

There are two levels of access available through the LDAP interface:

- [Anonymous subscriber directory access](#)
- [Trusted server access](#)

Anonymous subscriber directory access

Message Networking supports anonymous LDAP queries of its subscriber directory, which contains information about all the mailboxes in the enterprise, regardless of the type of remote machine used by each subscriber. Anonymous LDAP queries of the subscriber directory can be used in the following ways:

- Customer synchronization of the Message Networking Directory with other general enterprise directories (personnel directories)
- Third-party reporting application access to the Message Networking subscriber directory, including query of subscribers with recorded voice names
- Email client searches of employees within the enterprise

Note: Anonymous LDAP clients do not have to be administered in the Message Networking system to perform queries of the subscriber directory.

The document titled *LDAP Server Access* provides additional background and implementation information about accessing the LDAP server. In addition, the document *LDAP Schema for Message Networking* provides a list of the subscriber directory fields available through the LDAP interface and a list of recommended searches. Both of these documents are available from the [Avaya support site](#).

Trusted server access

A remote machine administered as an LDAP client, also called an LDAP trusted server, can access the Message Networking application for LDAP queries and system administration. An LDAP trusted server has special permission to perform query and administrative functions on the Message Networking system.

Note: If a remote machine is not administered as an LDAP client, all of the remote administration capabilities defined for the system are blocked except for anonymous subscriber directory access.

Customers can develop their own applications for LDAP access to the system, or you can contact your Avaya sales representative for information about third-party LDAP clients that support Message Networking's LDAP interface. If you choose to develop your own application, see *LDAP Server Access* for implementation information.

The following tasks can be performed through Message Networking's LDAP interface using an LDAP client administered as a trusted server:

- Anonymous queries of the subscriber directory
 - Queries of administrative and report data
 - Subscribers
 - Remote machines
 - Call detail recording
 - Traffic
 - Enterprise Lists
- Note:** As an alternative, you can use [FTP](#), [secure upload](#) or [secure download](#) to import subscriber directories or export reports that are saved in ASCII format.
- Outbound subscriber updates (based on directory view settings):
 - Adds
 - Changes
 - Deletes
 - Inbound subscriber updates for specific remote machine types:
 - AMIS
 - Serenade Octel Analog
 - VPIM
 - SMTP/MIME – non-Modular Messaging with an Avaya Message Storage System (MSS) and Avaya Aura™ Messaging
 - Administration of remote machine data:
 - Adds
 - Changes
 - Deletes
 - Enterprise List administration:
 - System administrator functions:
 - Administer at the system level and list level
 - Synchronize the enterprise personnel directory with the Enterprise List application
 - Implement third party applications that provide enhanced graphical user interfaces (GUIs) to administer and report on lists
 - Subscriber administration functions:
 - Create lists
 - Add, delete, and change entries in a given list
 - Self-subscribe to subscription-based Enterprise Lists
 - Access reports

Note: Subscriber access to these Enterprise List administrative functions depends on the permissions assigned to the subscriber on the Message Networking system. For more information, see [Administering subscriber permissions for LDAP Clients](#).

The document titled *LDAP Server Access*, which is available from the Avaya support site, provides a list of the subscriber directory fields available through the LDAP interface and a list of the recommended searches. Go to <http://www.avaya.com/support> and then navigate to the Message Networking page.

So that an LDAP client can access Message Networking through the LDAP interface, you must establish a

secure and trusted connection:

1. [Administer an LDAP client](#) remote machine for each LDAP client that will access the Message Networking system. The remote machine profile includes information such as the IP address of the LDAP client, the password that will be used to authenticate the connection, and whether automatic updates are supported to and from the LDAP client.
2. Once the LDAP client remote machine is administered, the remote client can request a connection from the Message Networking server. The LDAP client must supply a valid login (or domain name) and password. If the client's connection request is secured with a login and password, the system considers the connection to be from a trusted server.

If a connection request fails login and password verification, the connection is considered anonymous, and its search capabilities are limited to a subset of subscriber directory information. The system rejects any add, modify or delete requests by anonymous connections.

3. Message Networking supports SSL for both incoming and outgoing LDAP connections. Message Networking uses standard LDAP port 389 for LDAP client access. If you want to use SSL for LDAP transmissions, you must configure it on the LDAP client you are using. For Release 2.0 and earlier systems, there is no administration required on the Message Networking system to enable SSL for LDAP. See *LDAP Server Access* for additional information. For Release 3.1 and Release 5.2 systems, the Message Networking system can be administered to enforce SSL encryption for incoming directory updates.

Note: If you are using certain older versions of ldapsearch from the command line, and you want to use -ZZ, you must enter the fully qualified domain name (FQDN) for the host on which the LDAP server is running. Newer versions do not require you to enter the FQDN.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Message Networking system capacities



Message Networking system capacities

The following table shows the system capacities for a Message Networking system.

System attribute	S3210R system capacity	S3500-H system capacity	S3500 Basic system capacity	S8800 2U system capacity
Number of subscribers (network-wide)	500,000 (250,000 with voice names) Notes: <ul style="list-style-type: none"> The existence of any Message Networking systems that run on the S3210R server limits the number of network-wide subscribers with voiced names to 120,000. Modular Messaging and Avaya Aura™ Messaging systems do not support more than 250,000 subscribers (with or without voice names) during updates. Therefore, if the Message Networking system has more than 250,000 subscribers and you are updating to a Modular Messaging and Avaya 	500,000 (250,000 with voice names) Notes: <ul style="list-style-type: none"> The existence of any Message Networking systems that run on the S3500-H server limits the number of network-wide subscribers with voiced names to 120,000. Modular Messaging and Avaya Aura™ Messaging systems do not support more than 250,000 subscribers (with or without voice names) during updates. Therefore, if the Message Networking system has more than 250,000 subscribers and you are updating to a Modular Messaging and Avaya 	500,000 (250,000 with voice names) Notes: <ul style="list-style-type: none"> The existence of any Message Networking systems that run on an S3500 Basic server limit the number of network-wide subscribers with voiced names to 120,000. Modular Messaging and Avaya Aura™ Messaging systems do not support more than 250,000 subscribers (with or without voice names) during updates. If the Message Networking system has more than 250,000 subscribers and you are updating to a Modular Messaging and Avaya Aura™ 	500,000 (250,000 with voice names) Notes: <ul style="list-style-type: none"> The existence of any Message Networking systems that run on an S8800 2U server limit the number of network-wide subscribers with voiced names to 120,000. Modular Messaging and Avaya Aura™ Messaging systems do not support more than 250,000 subscribers (with or without voice names) during updates. If the Message Networking system has more than 250,000 subscribers and you are updating to a Modular Messaging and Avaya Aura™ Messaging remote machines, you must administer the Modular Messaging remote machine and Avaya Aura™ Messaging

	<p>Aura™ Messaging remote machines, you must administer the Modular Messaging remote machine and Avaya Aura™ Messaging remote machines to use directory view updates. The directory view that you administer for the Modular Messaging and Avaya Aura™ Messaging systems must not include more than 250,000 subscribers.</p>	<p>Aura™ Messaging remote machines, you must administer the Modular Messaging remote machine and Avaya Aura™ Messaging remote machines to use directory view updates. The directory view that you administer for the Modular Messaging and Avaya Aura™ Messaging systems must not include more than 250,000 subscribers.</p>	<p>Messaging remote machines, you must administer the Modular Messaging remote machine and Avaya Aura™ Messaging remote machines to use directory view updates. The directory view you administer for the Modular Messaging and Avaya Aura™ Messaging systems must not include more than 250,000 subscribers.</p>	<p>remote machines to use directory view updates. The directory view you administer for the Modular Messaging and Avaya Aura™ Messaging systems must not include more than 250,000 subscribers.</p>
<p>Number of remote machines per Message Networking. Note that due to traffic loads, it will be rare that the maximum of 500 will be reached.</p>	<p>500 (default of 1; average of 8 to 10)</p>	<p>500 (default of 500; average of 25)</p>	<p>500 (default of 1; average of 8 to 10)</p>	<p>500 (default of 500; average of 25)</p>
<p>SMTP Ports (includes VPIM and SMTP/MIME)</p>	<p>8 (default 0; possible values are 0 or 8)</p>	<p>20 (default 20; possible values are 0 or 20)</p>	<p>8 (default 0; possible values are 0 or 8)</p>	<p>20 (default 20; possible values are 0 or 20)</p>
<p>Aria Digital ports</p>	<p>4 (default 4)</p>	<p>16 (default 16)</p>	<p>4 (default 4)</p>	<p>16 (default 16)</p>
<p>Serenade Digital ports</p>	<p>4 (default 4)</p>	<p>16 (default 16)</p>	<p>4 (default 4)</p>	<p>16 (default 16)</p>
<p>AUDIX Digital TCP/IP Digital ports</p>	<p>4 (default 4)</p>	<p>12 (default 12)</p>	<p>4 (default 4)</p>	<p>12 (default 12)</p>
<p>Analog ports</p>	<p>4-port board (default 0; possible values</p>	<p>4-port board: 4 (default 4, possible</p>	<p>4-port board (default 0; possible values</p>	<p>4-port board: 4 (default 4, possible values are</p>

	are 0, 4, 8, or 12)	values are 0, 4) 12-port board: 12 (default 0; possible values are 0, 4, 12). Note: The S3500-H supports one 4-port analog board or one 12-port analog board.	are 0, 4, 8, or 12)	0, 4) 12-port board: 12 (default 4; possible values are 0, 4, 12). Note: The S8800 2U supports one 4-port analog board or one 12-port analog board.
Average message delivery time Note: The average message delivery time does not include the processing time at the sending and receiving systems. It also does not include the use of Enterprise Lists, which can be quite large and processor-intensive.	15 minutes	15 minutes	15 minutes	15 minutes
Call Detail Recording (CDR) records	100,000 (an average of 10,000 records per day for 10 days)	200,000 (an average of 20,000 records per day for 10 days)	100,000 (an average of 10,000 records per day for 10 days)	200,000 (an average of 20,000 records per day for 10 days)
Number of dial plan entries per remote machine	2,000	2,000	2,000	2,000
Performance See the note below the table for information about performance.	3,768 one-minute messages are supported (1,884 one-minute messages in and 1,884 one-minute messages out) during the network busy hour. The number of one-minute messages supported does not depend on the	9,808 one-minute messages are supported (4,904 one-minute messages in and 4,904 one-minute messages out) during the network busy hour. The number of one-minute messages supported does not depend on the	3,768 one-minute messages are supported (1,884 one-minute messages in and 1,884 one-minute messages out) during the network busy hour. The number of one-minute messages supported does not depend on the	9,808 one-minute messages are supported (4,904 one-minute messages in and 4,904 one-minute messages out) during the network busy hour. The number of one-minute messages supported does not depend on the sending or receiving encoding type.

	sending or receiving encoding type.	sending or receiving encoding type. Note: If the Message Networking system reaches the maximum supported traffic during the busy hour, <i>do not</i> perform updates to remote machine. In addition, if the Message Networking system reaches its during the time that the nightly audits run (which might occur on systems that experience heavy traffic with international systems), the audits might be affected.	sending or receiving encoding type.	Note: If the Message Networking system reaches the maximum supported traffic during the busy hour, <i>do not</i> perform updates to remote machine. In addition, if the Message Networking system reaches its busy hour during the time that the nightly audits run (which might occur on systems that experience heavy traffic with international systems), the audits might be affected.
--	-------------------------------------	--	-------------------------------------	---

Note: A number of factors can affect system performance, including:

- Normal message traffic
- Enterprise List traffic
- Message size
- Message types (voice, fax, text, binary)
- Enterprise List administration (static, dynamic, etc.)
- Number of Message Networking involved
- Remote machine performance
- Protocols involved (SMTP/MIME, VPIM, etc.)
- WAN performance
- Voice transcoding
- Other activities occurring on the Message Networking system (such as audits, reports, LDAP access, system administration)
- Remote machine errors (such as full mailboxes, nonexistent subscribers)
- Protocol delivery schedules (some can be modified from the defaults)

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Administrator interface



Administrator interface

Administration of the Message Networking system is performed through the Web-based administration menu and pages or via Message Networking's [LDAP interface](#).

The Message Networking system supports both local access and remote access **to administer the system**:

- Local access **to the system** is supported using the Message Networking system's dedicated monitor and keyboard, via the supplied browser.
- Remote access **to the system** is supported through the system's modem or **through** the LAN **using** a supported browser. Configurations and remote access sequences vary widely, depending on the site. You might need to refer to the documentation for your terminal or terminal emulator **for the procedure to remotely access the system** that applies to your situation.

Note: If you are installing or migrating to Message Networking Release 5.2, SAL is the preferred remote access mechanism that Avaya recommends. To activate the remote access using SAL, you must register your Modular Messaging system and the SAL gateway. For more information, see [Secure Access Link 1.5 Gateway Implementation Guide](#). Avaya field technicians can also help you with the SAL registration.

Caution! The Message Networking system allows more than one person to perform the same function on the same screen, for example, adding a subscriber to the Message Networking system database. However, if two people happen **to edit** the same subscriber's profile, only the changes made by the person who saves the screen last are written to the system database. The other person's changes are lost.

Tip: Depending on your terminal emulator, you might **not be able to view** some of the Message Networking screens **correctly**. **Make the** changes from the terminal emulator's Controls or **from the Options** menu. In particular, **turn** word wrap or wraparound **off**.

The following options are available from most of the pages:

- Save, Submit, Add (or another action) **options** that execute a command or make a system change.
- Help **option** that opens a separate browser window to display the applicable Help topic.
- Field name links that open a separate browser window to display the applicable field description.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting Started](#) > [Message Networking concepts and features](#) > Message Networking maintenance



Message Networking maintenance

The philosophy behind the maintenance of a Message Networking system is that the system provides a single point of reference for troubleshooting a problem, regardless of the system configuration. All applications use the same alarm log to report errors occurring within an application or in its interaction with other applications. The [alarm log](#) receives entries from all areas of the system (including the Message Networking-specific modules), prioritizes the alarms according to severity, and makes the alarms accessible.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > System security



System security

The telecommunication industry faces a growing threat of theft of customer services. Securing the telecommunications system and its networked equipment is and should be of prime importance to an organization. Diligent attention to system management and security can help reduce such risks considerably. The security information provided here informs owners of the steps that Avaya has taken to secure the Message Networking system. It describes how to use the system administration tools to minimize unauthorized intrusions and provides safeguards and measures that you should take to ensure that the Message Networking system operates in a secure manner.

Your responsibility for the security of your system

No telecommunication system can be entirely free from the risk of unauthorized use. Customers have ultimate control over the configuration and use of the product and are solely responsible for ensuring the security of their systems. Customers who administer and use the system can tailor the system to meet their unique needs and are in the best position to ensure that the system is secure to the fullest extent possible. Customers are responsible for keeping themselves informed of the latest relevant information for configuring their systems to prevent unauthorized use. System managers and administrators are also responsible for reading all the recommendations, installation instructions, and system administration documents provided with the product so that they can understand the features that can introduce risk and the steps that need to be taken to reduce that risk.

Avaya does not guarantee that this product is immune from or will prevent unauthorized use of telecommunication services or facilities accessed through or connected to it. Avaya will not be responsible for any damages or charges that result from either unauthorized use or from incorrect installations of the security patches that are made available from time to time. To aid in combating such crimes, Avaya intends to strengthen relationships with its customers and continue to support law enforcement officials in apprehending and successfully prosecuting those responsible.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending e-mail to securityalerts@avaya.com. Reported vulnerabilities are prioritized and investigated. Any corrective action resulting from the vulnerability investigation are posted at <http://support.avaya.com/security>. Whether or not immediate support is required, please report all toll fraud incidents perpetrated on Avaya services to Avaya Corporate Security. Avaya Corporate Security is available for product issue consultation, investigation support, law enforcement, and education programs.

The following table contains a list of security concerns addressed in this documentation. Click on the topics for more information.

Topic	Description
Security overview	Provides an overview of the Message Networking system and describes the major areas in which the customer-premises-based systems are vulnerable. It provides information on the general security measures that can be taken to discourage unauthorized usage.
Feature security	Provides an overview of security for Message Networking system features.
Physical security	Provides information on maintaining the security of the hardware components, preventing unauthorized access to the system console and documentation, and on running backups and securing backup media.

Telecommunication service thefts	Provides information on various toll fraud issues, such as toll fraud types, toll fraud occurrences, unauthorized system usages, fraudulent call transfers, voice mail fraud, automated attendant security. Also provides information on the steps that should be taken to prevent and minimize the occurrence of these types of frauds.
Adjuncts	Provides information on adjuncts such as Access Security Gateway (ASG) and Mailbox Manager and preventive measures to limit the risk of unauthorized usages of the system through these adjuncts.
Network security	Provides information on networking security of the Message Networking system.
Password administration	Provides information on password standards, password setting and naming conventions, and password administration.
Access mechanisms	Provides information on the various ways that you can access the Message Networking system and describes the security measures for these access mechanisms.
Virus and worm protection	Provides information on the recommended security measures against viruses and worms.
Security policy	Provides information on the security policy and the recommended best practices.
Security maintenance	Provides information on the security related maintenance activities for your system.
References	Provides information on the Avaya Toll Fraud Helplines and Security information on the Internet.

The Avaya Statement of Direction

To help customers make the best possible security-related decisions, Avaya commits to the following:

- Avaya products and services will offer the widest range of options available in the industry to help customers secure their communications systems in ways consistent with their telecommunications needs.
- Avaya is committed to develop and offer services that, for a fee, reduce or eliminate customer liability for PBX toll fraud, provided the customer implements prescribed security requirements in its telecommunications systems.
- Avaya's product and service literature, marketing information, and contractual documents address, wherever practical, the security features of our offerings and their limitations, and the responsibility our customers have for preventing fraudulent use of their Avaya products and services.
- Avaya sales and service people are the best informed in the industry on how to help customers manage their systems securely. In ongoing contacts with customers, they will provide the latest and the most effective security-related information.
- Avaya trains its sales, installation and maintenance, and technical support people to focus customers on known toll fraud risks, to describe mechanisms that reduce those risks, to discuss the tradeoffs between enhanced security and diminished ease of use and flexibility, and to ensure that customers understand their role in the decision making process and their corresponding financial responsibility for fraudulent use of their telecommunications system.
- Avaya provides education programs to keep customers and Avaya employees apprised of emerging technologies, trends, and options in the area of telecommunications fraud.
- Avaya promptly initiates ways to impede new fraudulent schemes as they are developed, share our learning with our customers, and work with law enforcement officials to identify and prosecute fraudulent users whenever possible.
- Avaya intends to meet and exceed customer expectations, and provide services and products that are

easy to use and that are of high value. This fundamental principle drives our renewed assault on fraudulent usage by third parties of our customers' communications services and products.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Security overview



Security overview

This topic provides an overview of Message Networking security.

Security elements with Message Networking

Security concerns for the Message Networking system include toll fraud, unauthorized reprogramming of computer systems, unauthorized access to telecommunication system by misusing the call transfer capabilities of the system *or* through ports meant for remote administration or maintenance, unintended disclosure of confidential information, and virus attacks. These activities result in huge telephone bills, revenue loss, administrative costs, decreased system performance, and loss of customer confidence. The various security risks faced by telecommunication systems today are described in the following sections.

Telecommunications Fraud

Toll Fraud is a significant security concern in traditional voice messaging systems. Unauthorized people use personal computers, random number generators and password cracking programs to break into the most sophisticated systems and commit frauds. Today, with the convergence of voice and data and the advent of IP Telephony, security problems are not limited to toll fraud and unauthorized access. The advancement in technology has opened up a wide array of vulnerabilities that can compromise the security of the entire organization. See [Telecommunication service thefts](#) for more information on Toll Fraud.

Internal threats

Securing a system does not begin with the system itself, but with the people and organizations that use it. In deciding who to protect the system against, one must not forget to look internally. A significant number of attacks come from within. Internal security is important to the protection of information and assets. It is easier to misuse or damage the system by physical methods than by hacking the system passwords. Employees can easily access the mailbox of another employee and pass critical and confidential information, such as passwords, to unauthorized people. It is necessary to enforce a proper security policy against such internal breach of communications.

Internet threats

Message Networking is deployed into the existing corporate LAN and is exposed to the Internet. Security is a primary concern when an organization connects its network to the Internet. Network administrators have increasing concerns about the security of their networks when they expose their organization's private data and networking infrastructure to Internet crackers. Some of the common methods of attacks from the Internet include Internet worms, virus attacks, malicious e-mail attachments, IP spoofing, password attacks, network packet sniffers, Denial of Service attacks, and Application layer attacks. These attacks can lead to theft, and to destruction and corruption that can cause irreparable damage to sensitive and confidential information.

What you need to do

It is extremely important that system managers and administrators plan and implement the necessary security measures and ensure that:

- Message Networking integrates into your existing TCP/IP network in accordance with the corporate networking policies, and the server also allows the usage of existing firewall and of corporate security

policies and practices.

- The network prevents exposure of potentially sensitive customer messages by using sending restrictions that provide data for you to check to ensure that there has been no unauthorized usage.
- You prevent unauthorized use of the server capabilities by protecting the server with administrator and user passwords. Lengthy and random passwords minimize the possibility of hacking.
- The network prevents unauthorized command-line access to the main server.
- The network prevents all well known types of hacker attacks, including denial of service attacks.
- The servers provide sufficient logs, like the Administration History Log, to facilitate detection of actual and attempted unauthorized usage and identification of sources of unauthorized usage.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Feature security



Feature security

This topic provides security information for the following Message Networking features:

- [FTP](#)
- [HTTP/SSL](#)
- [Enterprise Lists](#)
- [CDR](#)
- [SMTP access](#)
- [LDAP](#)
- [SNMP](#)
- [Network access](#)
- [Network messages](#)
- [Network protocols](#)
- [Security enhancements for Release 5.2](#)

FTP

Message Networking provides authenticated FTP access for specific applications, including the following:

- Subscriber Imports
- Enterprise List Imports
- Report Exports
- CDR Exports
- Customer Downloadable Service Packs (software updates)

FTP access into Message Networking requires the use of the icftp login ID and password. This login ID is set to a default value when the Message Networking system is initially installed, but you are required to change the password during system administration.

FTP access in Message Networking is limited to the /iclog/icftp directory. This directory has a budgeted maximum amount of storage that cannot be exceeded by the FTP user. That is, importing more data than can be stored is prevented by the Message Networking system.

Message Networking systems are shipped with the FTP feature deactivated by default. If you activate FTP to use it for a task, such as exporting a report, it is recommended that you deactivate it when you complete the task.

HTTP/SSL

Message Networking provides secure file transfer to and from the Message Networking server using HTTP/SSL. These files are used for administering Enterprise Lists and Subscriber Lists and downloading reports.

Enterprise Lists

The administration of Enterprise Lists is limited to administrators logged into the Message Networking system and applications accessing the Message Networking LDAP interface (see [LDAP](#) for security considerations for the Message Networking LDAP server).

Senders must know the list ID network address (or corresponding ASCII name) of the list to which they want to send a message, and the sender's network address must be granted permission to use the list by the administrator.

CDR

Message Networking provides a seven-day cyclical file that records all information about the messages that pass through the system. This file is not a copy of the actual message (messages are transient and the system deletes them after delivery), but is a record that the message was sent.

Access to this information requires administrative system access (tsc, sa, craft, dadmin, and icftp logins).

The CDR feature has actually been used in the past by system administrators to track and capture unauthorized users that gained access to a remote machine server mailbox and sent disruptive messages from that mailbox.

SMTP access

The Message Networking supports exchange of messages to and from other remote systems that support secure SMTP with the secure socket layer (SSL) encryption.

The Message Networking allows you to receive the incoming messages through one of the following method:

- standard SMTP on a default TCP/IP port 25
- secure SMTP on a default TCP/IP port 465
- both the standard and secure SMTP on a custom port.

For outgoing messages, you can configure the standard SMTP or secure SMTP from the Message Networking administration Web interface.

LDAP

Message Networking uses LDAP for updates between Message Networking systems, Modular Messaging and Avaya Aura™ Messaging systems (using port 56389). Message Networking also provides an LDAP-based interface (using standard LDAP port 389) that can be used to obtain directory data. The Message Networking LDAP-based interface requires authenticated access. If you are not using SSL for LDAP, the version of LDAP supported is the standard, unencrypted, version, and any adjunct processors using authenticated LDAP will transmit their login credentials in plain text, so security of the link between these processors and the server is important.

Message Networking supports SSL for both incoming and outgoing LDAP client connections. Message Networking uses standard LDAP port 389 for LDAP client access. If you want to use SSL for LDAP transmissions, you must configure it on the LDAP client you are using. For Release 2.0 and earlier systems, there is no administration required on the Message Networking system to enable SSL for LDAP. See *LDAP Server Access* for additional information. For Release 3.1 and later systems, the Message Networking system can be administered to enforce SSL encryption for incoming directory updates.

Note: If you are using certain older versions of `ldapsearch` from the command line, and you want to use `-ZZ`, you must enter the fully qualified domain name (FQDN) for the host on which the LDAP server is running. Newer versions do not require you to enter the FQDN.

SNMP

SNMP, the current working standard of the TCP/IP protocol suite, is used to transfer network management information. Through SNMP, various elements of a network can communicate with each other regardless of their underlying architecture. Message Networking supports its own implementation of SNMP, which allows network system administrators to monitor remote Message Networking elements from a central location.

The Message Networking system supports SNMP versions 2c and 3. For version 2c, the network management station uses community strings to secure access to SNMP information. For version 3, the network management station uses views to secure access to SNMP information. See [Simple Network Management Protocol overview](#) for more information on SNMP on Message Networking.

System access

Message Networking does not allow subscribers into the server for mailbox access. Message Networking strictly serves as a postmaster, receiving and sending networked messages. The only login access to the system is by system administrators using the standard login IDs (for example, sa, craft).

Message Networking provides a secure Web connection that requires the administrator's browser to have a [security certificate](#).

Network messages

Access to all messages processed by Message Networking require the following:

- tsc login access
- Knowledge of the directories where the actual messages are stored.
- A process that continuously monitors the system (Message Networking messages are transient and deleted from the system once delivered).
- A transcoder or player for each of the voice formats supported by the system (proprietary and non-proprietary).

Network protocols

The following table lists the networking protocols supported by Message Networking and the security-related considerations for each.

Protocol	Security considerations
AMIS	<ul style="list-style-type: none"> • Standard protocol. • Requires authentication of Callback Number on both ends. • Requires proper military tone sequence for session setup. • Actually plays voice message over analog line.
Octel Analog Networking	<ul style="list-style-type: none"> • Proprietary protocol. • Requires authentication of Octel Serial Number on both ends. • Supports encryption of touch-tone values. • Requires proper military tone sequence for session setup. • Actually plays voice message over analog line.
AUDIX Digital	<ul style="list-style-type: none"> • Proprietary protocol. • Uses port 5500 (listen port). • Uses CELP voice encoding (proprietary).

	<ul style="list-style-type: none"> • Requires authentication of password and machine name on both ends.
Aria Digital	<ul style="list-style-type: none"> • Proprietary protocol. • Uses port 4000 (listen port). • Uses SBC voice encoding (proprietary). • Requires authentication of Octel Serial Number on both ends.
Serenade Digital	<ul style="list-style-type: none"> • Proprietary protocol. • Uses port 22136 (listen port). • Requires IP address of both systems to be administered on each end. • Does not have any password authentication. • Uses CVSD voice encoding (proprietary).
SMTP/MIME	<ul style="list-style-type: none"> • Standard protocol. Also supports secure protocol SMTP/SSL. • Refer to the general notes in this document regarding SMTP/MIME Internet access. • Standard SMTP protocol uses port 25 and the secure SMTP protocol uses port 465. You can use custom port for both the protocols. • Uses GSM. G.711 (mu and A law) voice encoding. <p>Note: Message Networking Release 5.2 supports standard SMTP, secure SMTP, or Both for incoming messages. For outgoing messages, you can configure Standard SMTP or Secure SMTP from the Remote Machine menu on the Message Networking administration Web interface.</p>
LDAP-Based Subscriber Directory Updates	<ul style="list-style-type: none"> • Subscriber directory updates based on LDAP. • Provides directory adds/changes/deletes. • Has an all directory pull and push capability. • For Message Networking, port 56389 is used. • For MMA, port 55389 is used.
VPIMv2	<ul style="list-style-type: none"> • Standard protocol. • See SMTP/MIME (uses port 25). • Uses ADPCM voice encoding.
LDAP server access	<ul style="list-style-type: none"> • Standard protocol. • Uses port 389.

Security enhancements

The following security enhancements have been added to Message Networking Release 5.2:

- [Stringent Password rules](#)
- [Message exchange using standard SMTP, secure SMTP, or both](#)
- [File transfer using HTTPS/SSL encryption](#)
- [AAA LDAP plain password encryption](#)

Stringent Password rules

To improve control over access to the Message Networking system, an administrator can specify more stringent password rules to the group of locally-authenticated system accounts.

Message exchange through standard or secure SMTP

Exchange of messages to and from other remote systems that support secure SMTP with the secure socket layer (SSL) encryption.

File transfer using HTTPS/SSL encryption

The Message Networking ensures secure file transfer from and to the Message Networking server. The Message Networking provides menus from the from the Message Networking administration Web interface for the secure file transfer.

AAA LDAP plain password encryption

AAA LDAP server supports encryption of login credentials in plain text. The encrypted password is stored in *.aaaconfig.ldappwd* file.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Physical security

Physical security

Ensuring the physical security of all the hardware components must be an important consideration in securing your Message Networking system.

General recommendations

- You should always limit access to the system console and to the supporting documentation.
- Provide good physical security for the room that contains the telecommunications equipment, administrative tools, records, system programming, and other vital information. Make sensitive areas physically secure during unattended times using methods such as locked doors or automatic detection devices.
- Establish and maintain a clear physical perimeter.
- Ensure that you restrict access to server rooms and lock these rooms when not attended. Access to work areas should be strictly limited to authorized personnel only.
- Keep the attendant console and supporting documentation in a place that is secured with a changeable combination lock. Provide the combination to only those individuals have a real need to access the premises.
- Keep telephone wiring closets and equipment rooms locked.
- Keep telephone logs and printed reports in locations that only authorized personnel can access.
- Design distributed reports so that they do not reveal password or trunk access code information.
- Provide secure trash disposal for all sensitive information, including telephone directories, call accounting records, or anything that may supply information about your communications system. Such trash should be shredded.
- Schedule regular backups for the Message Networking system. This will ensure timely recovery when recovery is required. See [Backing up and restoring the system](#) for more information.

Backups

Unfortunately, backups are frequently not included when security lists are made. Even at large organizations the importance of testing backups is sometimes neglected. A backup plan is necessary to ensure that essential, electronically stored business data can be recovered in the event of a system failure or disaster. Ensure that you develop and implement proper backup procedures for the system. Also create a data backup of all those machines that should be backed up such as a desktop system with valuable data. Backups must cover more than a few days so that older versions of files can be recovered and so that there is a reasonable chance of recovering from problems, especially intruder-caused damage that goes undetected for a significant time.

Without good backups, hardware failures might cause irretrievable data loss, and recovering from an intrusion might be difficult. Back up system files regularly to ensure a timely recovery should it be required. Schedule regular, off-site backups, periodically tested, with reasonable media rotation and offsite storage. See [Backing up and restoring the system](#) for more information on backup procedures for the Message Networking system.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Telecommunication service thefts



Telecommunication service thefts

The telecommunication industry faces a growing threat of theft of customer services. No telecommunications system can be totally free from the risk of unauthorized usages. Insuring that your systems are maintained in a secure manner is therefore a prime responsibility of each organization. This section provides information on toll fraud and service theft, and on ways to use the system administration tools to minimize the possibility of such unauthorized activities occurring on your system.

The following topics are included:

[Toll fraud](#)

- [What is Toll Fraud?](#)
- [How does Toll Fraud occur?](#)

[Detecting Toll Fraud](#)

[Unauthorized system use](#)

Toll Fraud

Toll fraud is one of the most expensive corporate crimes that poses a major threat to telecommunication systems. Toll frauds can result in huge phone bills, revenue loss in terms of its operational impact, additional expenses, service interruptions, and the most important of them all, loss of customer confidence.

What is Toll Fraud?

Toll Fraud is the unauthorized use of a company's telecommunications service by an unauthorized party (for example, a person who is not a corporate employee, an agent, or a subcontractor). It occurs when people misdirect their own telecommunications charges to another person or business.

How does Toll Fraud occur?

Toll fraud is possible when your system allows the incoming caller to make a network connection with another person. It is therefore important to protect vulnerable areas such as call transfer and bridging to an outbound call. There are numerous ways in which unauthorized users can attempt to breach your system security. These include:

- **Unauthorized system use.** Intruders access one of your messaging systems, create a mailbox, and use the system. Hackers use personal computers, random number generators, and password cracking programs to break into customer premises equipment-based systems. Hackers continuously dial into the PBX or telephone equipment and probe the system for a weakness that will provide access to an outside line. Once an outside line is obtained, long distance calls are made.
- **Unauthorized use of AMIS Analog Networking call delivery.** An intruder uses your system to send an AMIS message or a fax to a distant number or someone who is already in your system is making unauthorized calls. The unauthorized usage could be from an employee, or from someone who has breached your system security and gained access. To minimize the security risk of AMIS Analog Networking, restrict the number ranges that can be used to address messages. Be sure to assign all the appropriate PBX outgoing call restrictions on the voice ports.

Warning! Toll fraud is a theft of long distance service. When toll fraud occurs, your organization is responsible for the charges incurred. Call Avaya's Customer Care Center, 1-800-643-2353 for more information on how to prevent toll fraud.

Detecting Toll Fraud

To detect possible hacker activity on the Message Networking system, you can use system traffic reports to track system traffic data over various time periods. Reviewing these reports on a regular basis helps to establish traffic trends. If increased activity or unusual usage patterns occur, such as heavy call volume on ports assigned to outcalling, they can be investigated immediately. You can also use the Server Events Log and Activity Log to monitor usage and investigate possible break-in attempts. For more information on running and using reports, see [Reports](#).

Unauthorized system use

To minimize the risk of unauthorized break-ins to the system, strictly follow the compliance guidelines for your system administration and trusted server passwords, and use the password aging feature.

Modular Messaging comes with administrative password features and options that assist you in securing your system. These include:

- **Changing default administrator password.** When you first get your system, make sure that you change the system administrator login password immediately.
- **Administrator password standards.** You must follow the minimum password standards to comply with the system's standards.
- **Administrator password aging.** Use the password aging feature parameters to enhance the security levels of the system. This will ensure that administration passwords are changed at regular intervals. You can also use the password expiration feature for administrative logins to reduce the danger of unauthorized access.

See [Administering passwords](#) for more information on passwords.

You can ensure additional security by using the Avaya Access Security Gateway (ASG) guard which is used to provide secure remote access to the Message Networking system. See [Adjuncts](#) for more information on ASG.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Security of system adjuncts



Security of system adjuncts

This topic provides information about the security of Message Networking system adjuncts.

Access Security Gateway (ASG)

The Access Security Gateway (ASG) feature is an optional authentication interface you can use to secure the sa login on the Message Networking system. Whenever a dial-up port user begins a session on the system for purposes of administration or maintenance, the user must enter a valid login ID. If the ASG interface is activated, the system issues a numerical challenge. To access the Message Networking administration and maintenance features, the user must enter the correct numerical response. By activating the ASG feature, you can reduce the possibility of unauthorized remote access to the system.

You administer ASG parameters to specify whether access to the system requires ASG authentication. You can assign this protection to all system administration maintenance ports or to a subset of those ports. If the port or login being used is not protected by ASG, the user can enter the system with the standard Message Networking login and password.

The following procedure describes how the ASG interface works:

1. At the beginning of a login session, a message asks the user to enter a login ID.
2. Upon receipt of the login ID, ASG generates a number based upon the system ASG secret key number and presents this 7-digit number as a challenge.
3. The user must have a handheld device, called the ASG Key. The ASG Key must be set with an ASG secret key number that matches that of the user's ASG secret key number in the Message Networking system.
4. The user enters the PIN and challenge number into the ASG Key.
5. The ASG Key generates and displays a unique, 7-digit numerical response that corresponds to the challenge number.
6. The user enters the response number at the `response:` prompt.
7. If the response supplied by the user:
 - o corresponds to the numerical response expected by the Message Networking system, the authentication is successful and the user is logged in to the system.
 - o does not correspond to the numerical response expected by the Message Networking system, the user is not authenticated and is denied access to the system. The failed authentication attempt is recorded in the system history log.

Note: The system administrator determines how many login attempts are permitted. If the user is not authenticated after that number of attempts, the system displays the message `INVALID LOGIN` and terminates the session.

To administer ASG on Message Networking, see [Administering the Access Security Gateway \(ASG\)](#).

LDAP client

Message Networking supports the use of [LDAP client](#) machines to extract information from and perform administration of the Message Networking system.

LDAP clients connect to Message Networking through a trusted server connection on the Message Networking

system. The machine running the LDAP client must be administered as an [LDAP client remote machine](#). An LDAP password is used to increase security. Make sure that the password is at least eight characters and is not composed of easily guessed words or numeric combinations.

It is advisable that all logins to the LDAP client should be password protected. It is important that you do not leave any desktop or laptop machine that has an LDAP client installed unattended, even for a little while. Make sure that you lock your computer every time you are not working on it. This will prevent any unauthorized access to the LDAP client. It is also advisable to change the passwords on a regular basis as unauthorized people may obtain documentation copies of your system and adjuncts and circulate the administrative passwords to gain entry into your systems.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Network security



Network security

The Message Networking system is designed to be located securely within the network and should not be directly connected to the Internet. You should leverage the existing network security policy to protect the system from malicious activities from external and internal sources. Although protecting information may be a high priority, protecting the integrity of your network should not be less important. When your network is connected to the Internet, it is exposed to various types attacks including Network packet sniffers, IP spoofing, password attacks, Denial-of-service attacks, and application layer attacks. A breach of integrity can be extremely dangerous and can open the doors for continued attacks on your system. Your network, security and applications teams should work together to plan and manage security. You should consider the measures described below for reducing security risks when deploying the Message Networking system into your network.

Internet firewalls

An Internet firewall is a system or a group of systems that enforces a security barrier between your network and the Internet. The firewall determines which inside services can be accessed from outside and which outside services can be accessed by insiders. Because the Message Networking server will be implemented as an e-mail receiver, the customer site must have a firewall between the Message Networking server and the Internet.

To properly secure FTP access into the Message Networking system, access to the FTP port (21) outside of the firewall must be prohibited.

It is also advisable to explicitly identify the untrusted networks from which the firewall can accept requests. Ensure that all the traffic to and from the Internet passes through the firewall.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) can be used for detecting unauthorized break-ins to your systems. It is advisable to implement a network-based intrusion detection system as a secondary security system. Following are some of the reasons for adding an IDS to your network. IDS:

- Cross-checks incorrectly configured firewalls
- Detects attacks that firewalls legitimately allow through (such as attacks against Web servers)
- Detects failed hacking attempts to get into your system
- Detects insider hacking

Trusted Server

A trusted server for Message Networking is an LDAP client that is given privileged access to Message Networking's LDAP server. The first step in securing the system is to make certain that only trusted systems are working together.

[Top of page](#)

.





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Administration](#) > [Accessing the system](#) > Administering passwords



Administering passwords

This topic provides information on administering the passwords used to control access to the system.

Use the procedures in this topic to:

- administer the password rules
- change the password for a login
- set the interval at which the system passwords must be changed.

Overview of passwords

Access to the Message Networking system is controlled by a set of passwords that provide different access levels. The following administration accounts (also called logins) are provided with the system for system installers, administrators, and support personnel:

- **sa:** The *sa* login is for use by the customer's system administrators either from the console or from another computer on the customer's LAN.
- **craft:** The *craft* login is for use by Avaya personnel performing system installation, administration, or maintenance on the customer site, either from the console or from another computer on the customer's LAN.
- **dadmin:** The *dadmin* login is for use by Avaya Business Partners performing administration or maintenance on the customer site, either from the console or from another computer on the customer's LAN. The customer must use the *craft* login to activate the *dadmin* login and grant permission. The *dadmin* login has the same permissions as the *craft* login.
- **icftp:** The *icftp* login is for use with Message Networking's secure [file upload](#) , secure [file download](#) and [FTP features](#). These features enable file importing and exporting.
- **sappp:** The *sappp* login is for use by a system administrator performing system administration and maintenance remotely using a dial-up connection. You must set up the *sappp* password to allow a remote administrator to dial in to the system.
- **craftppp:** The *craftppp* login is for use by remote Avaya personnel performing system installation, administration, or maintenance using a dial-up connection. You must set up the *craftppp* password to allow Avaya personnel to dial in to the system.

When your system is installed, the *sa* and *icftp* logins come with default passwords. You must change these passwords immediately to ensure system security following minimum password standards. You must also set up the system's PPP logins, to allow a remote service center to dial in to the system to perform troubleshooting or system maintenance. For information on setting up these logins, see [Administering logins and passwords](#).

In addition to the administration accounts that are available after the system is installed, you can use the *sa* login to create new administration accounts for logging in to the system either from the console or from another computer on the customer's LAN. The administration accounts you create can have access privileges that are the same as the *sa* account, or you can create administration accounts that have different access privileges. For more information, see [Managing local administration accounts](#).

To create administration accounts that have access privileges that are different from the *sa* account, you first have to set up one or more administrative roles. When you set up an administrative role, you specify which web-administration pages the role can access and the access type. For more information about setting up administrative roles, see [Role-Based Access Control](#) and [Managing administrative roles](#).

When you create administration accounts, you can specify whether the account is authenticated locally when a

user logs in to the system. Administration accounts can also be authenticated by an Authentication, Authorization, and Accounting (AAA) server, if one has been configured. For more information, see [Configuring the system for login authentication by an AAA server](#).

Additionally, you can administer several parameters of the password aging feature that will enhance the level of security the system maintains.

Note: You can [administer the Access Security Gateway \(ASG\)](#) on the Message Networking system to provide additional security. The ASG provides strong authentication for the Message Networking system logins by challenging each potential dial-up session user when the authentication type for a particular login is set to ASG. To respond to the ASG challenge, the user must have a handheld device, called the ASG Key, which must be set with an ASG secret key number that matches that of the user's ASG secret key number in the Message Networking system.

Guidelines for passwords

To minimize the risk of unauthorized people using the Message Networking system, follow these guidelines for system passwords.

- Establish a new password as soon as the Message Networking system is installed.
- Use a password containing at least 6 alphanumeric characters. See Password Rules Administration.
- Never use obvious passwords, such as a telephone extension, room number, employee identification number, social security number, or easily guessed numeric or letter combinations.
- Do not post, share, print, or write down passwords.
- Do not put the password on a programmable function key.
- Change the password at least once per month. You can administer your system to age the password and notify you that a new password is required. For more information, see [Setting administrator password aging](#).
- If you suspect that the security of any password has been compromised, notify your project manager or system administrator.

Administering password rules

Only administrators who have access to the **Password Rules Administration** page can administer the password rules. You can use the **Administrative Roles** menu under **Security** to provide the permission to administer the password rules.

To set the password rules, the administrator must complete the following fields:

1. On the Administration menu, under **Security**, click **Password Rules**.
The system displays the **Password Rules Administration** page. For information about the fields on this page, click **Help**.
2. Complete the following fields:
 1. **Minimum Password Length:** Specify a number between 6 and 16. The default is 8 characters.
 2. **Number of Previous Passwords That Must Not Match:** Specify a number between 0 and 12. The system keeps a record of the previous passwords and checks against them based on the value you specify. The default is 1. For example, if you set the value to **3**, the new password must not match any of the previous three passwords.
 3. **Passwords Must Contain at Least this Many of the Selected Types of Characters:** Specify the minimum number of character types a password must have. Select a value between one and four. Ensure that the number of character types selected is equal to or greater than the value specified. The default is 2 and the character types selected are *Lowercase* and *Numbers*.
 - **Lowercase (a-z):** If selected, the password must contain at least one lowercase alphabetic character from [a - z].
 - **Uppercase (A-Z):** If selected, the password must contain at least one uppercase alphabetic character from [A - Z].

- **Numbers (0-9):** If selected, the password must contain at least one numeric value from [0 - 9].
 - **Special Characters (@ % ~ - _ / + = . ? [] { } ! ^ * : , ;):** If selected, the password must contain at least one special character. The system supports [@ % ~ - _ / + = . ? [] { } ! ^ * : , ;] characters.
4. **Number of Failed Login Attempts Before Account Lockout:** Specify a number between zero and five. The default is 0, which means the account does not get locked with any number of failed login attempts.
- If you set a value between one and five, the system keeps a track of the number of consecutive failed login attempts. The system denies access if the count of failed attempts exceed the value set by the administrator. For example, if you set to 4, and five consecutive login attempts fail, the account gets locked. The system unlocks the account automatically in 10 minutes.

3. Click **Save**.

Changing passwords

You must immediately change the password for the *sa*, *icftp*, *craft*, and *dadmin* logins after your system is installed. Once a new password is established, you must also establish a regular schedule for changing the password, for example, at least monthly. Be sure to alert any other Message Networking administrators or system administrators after a password is changed.

The logins for which you can change the password depend on your login. For example, when you log in using the *sa* login, you can change the password for the *sa*, *icftp*, and *sapp* logins. Every user can change the password associated with their own administration account (login).

To change the password for a local administration account (login):

1. In the Administration menu, under **Security**, click **Local Administrators**.
The system displays the **Manage Local Administration Accounts** page. For information about the fields on this page, click **Help**.
2. Select the login for the password you want to change.
3. Click **Edit the Selected Admin**.
4. In the **Password** field, type a new password. The new password should conform to the password rules set by the administrator in the [Password Rules Administration](#) page. If the **Local Authentication Enabled?** field is set to yes, a password must be entered for this local administration account.
5. In the **Confirm Password** field, type the new password again for verification.
6. Select the **Change Password at next Logon** field, to change the password when you log in to the Message Networking admin.
7. Click **Save**.

To change the password for the *icftp* login:

1. In the Administration menu, under **Security**, click **icftp Configuration**.
The system displays the **icftp Configuration** page. For information about the fields on this page, click **Help**.
2. In the **Local Authentication Enabled?** field, select **yes** if you want this login to be authenticated by the Message Networking system, select **no** if you want this login authenticated by an external AAA server.
3. In the **New Password** field, type a new password. The new password should conform to the password rules set by the administrator in the [Password Rules Administration](#) page.
4. In the **Confirm Password** field, type the new password again for verification.
5. Click **Save**.

To change the password for your local administration account (login):

1. In the Administration menu, under **Security**, click **Change My Password**.
The system displays the **Change My Password** page. For information about the fields on this page, click **Help**.
2. In the **Old Password** field, type your current password.

3. In the **New Password** field, type a new password containing. The new password should conform to the password rules set by the administrator in the [Password Rules Administration](#) page.
4. In the **Confirm Password** field, type the new password again for verification.
5. Click **Save**.

Setting Administrator Password Aging

You can determine how often the system's passwords have to be changed by setting Password Aging parameters. The logins for which you can set Password Aging parameters depend on your login. For example, when you log in using the `sa` login, you can set Password Aging parameters for the `sa`, `icftp`, and `sapp` passwords. Avaya recommends that you set Password Aging parameters to help maintain a high level of system security.

To set Password Aging parameters:

1. In the Administration menu, under **Security**, click **Local Administrators**.
The system displays the **Manage Local Administration Accounts** page. For information about the fields on this page, click **Help**.
2. Select the login for which you want to set Password Aging parameters.
3. Click **Edit the Selected Admin**.
The system displays the **Edit Local Administration Accounts** page.
4. Complete the following fields:
 1. **Password Expiration**: Select **Enabled** or **Disabled**. If the **Password Expiration** field is set to **Enabled**, in the days field, type the number of days a password can be valid/active before the user is forced to change it. The default value for the **Password Expiration** field is **Disabled**. The range for the days field is 1 through 9999. The default value for the days field is 90.
 2. **Minimum Age Before Changes**: Select **Enabled** or **Disabled**. If the **Minimum Age Before Changes** field is set to **Enabled**, in the days field, enter the number of days before the user can change the password. You cannot change the password until the value specified in the days field has elapsed. For example, if you enter '5' in the days field, you cannot change the password for next 5 days.
If the **Minimum Age Before Changes** field is set to **Disabled**, you can change the password as frequently as desired. By default, the **Minimum Age Before Changes** field is set to **Disabled**. The range for the **Minimum Age Before Changes** days field is 1 through 999. Note: The value you specify for the **Minimum Age Before Changes** days field must be less than or equal to the value you specify for the Password Expiration, days field.
 3. **Expiration Warning**: Select **Enabled** or **Disabled**. If the **Expiration Warning** field is set to **Enabled**, in the days field, specify the number of days prior to password expiration that the expiration warning begins to display. At login, the system then displays a warning message that the password is scheduled to expire. When this message begins to appear depends on the value entered in the Expiration Warning, days field. For example, if you enter 5 in the Expiration Warning, days field, the expiration warning message begins to appear five days before the password expires, and continues displaying until the password is changed. By default, the **Expiration Warning** field is set to **Enabled** and days field is set to 10. You can set the Expiration Warning, days field to a value from 1 through 30.
If the **Expiration Warning** field is set to **Disabled**, the system does not display an expiration warning message to change the password before the password gets expired.
Note: The value you specify for the Expiration Warning, days field must be less than or equal to the value specified for the **Password Expiration**, days field.
 4. Select the **Change Password at next Logon** field, to change the password when you log in to the Message Networking admin.
5. Click **Save**.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Access mechanisms



Access mechanisms

Message Networking supports various access mechanisms, depending on the way it is configured.

Message Networking does not allow subscribers into the server for mailbox access. Message Networking strictly serves as a postmaster, receiving and sending networked messages. The only login access to the system is by system administrators using the standard login IDs (for example, sa, craft). See [Administering passwords](#) for a list of the login IDs supported by Message Networking.

Message Networking provides a secure Web connection that requires the administrator's browser to have a [security certificate](#).

Message Networking servers provide dial-up modem access, which is used by Avaya services personnel for troubleshooting and maintenance. This modem can be accessed by only those users who are added to the Avaya services group. These access restrictions are regulated by Avaya. Message Networking supports Secure Shell (SSH) for remote login access and file transfer over a LAN. All transmissions through this channel are encrypted using Secure Shell or Secure Socket Shell (SSH).

The Message Networking system (S3500-H server only) also includes an onboard Remote Maintenance Board (RMB) that provides dial-up modem access to the Avaya services personnel. Access to this modem is controlled by the Access Security Gateway (ASG) that employs a challenge and response mechanism for authentication. ASG reduces the possibility of unauthorized remote access to the Message Networking system. See [Adjuncts](#) for more information on ASG. It is strongly recommended that customers invest in security adjuncts, that typically use one-time pass code algorithms. These security adjuncts discourage hackers.

You can also set up a Point-to-Point (PPP) server for remote access to the Message Networking system. PPP service can be configured to enable remote access for local and remote machines. It is necessary for administrators to administer point-to-point protocol logins and passwords for the system. PPP logins are mainly used for maintenance. See [Administering logins and passwords](#) for more information on how to administer PPP logins.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Virus and worm protection



Virus and worm protection

Viruses and worms are targeted mainly at the operating systems. Viruses are most commonly transferred through e-mail, in the form of binary file attachments, through infected Web sites, or through shared disk drives on the network.

Message Networking supports the SMTP/MIME protocol. Message Networking system only allows authorized files to be sent as attachments between Message Networking and Modular Messaging systems. Additionally, the system administrator at the customer site **must** implement firewalls and Access Control Lists on the gateway routers to block any SMTP traffic from external sources.

Avaya recommends that you implement an anti-virus protection software directly on the corporate e-mail servers and on individual user systems to detect any SMTP/MIME viruses. Anti-virus detection may also be run on the Message Networking system at regular intervals. Infected files, if detected, should be cleaned or removed and restored from the backup.

Message Networking supports the download of software updates from the Avaya support site. It is critical that the machine to which you download Message Networking software updates have the latest virus detection software installed.

Anti-virus Software

Customer must carefully evaluate the security risks of email and file attachments **and make provisions for virus detection software that can sit between the Message Networking server and incoming email.** Your PC/LAN administrator should be able to advise on how your LAN is already set up or could be set up to detect and prevent the transmission of software viruses. At a minimum, you should advise your subscribers that file attachments should be detached (not launched) and scanned for viruses before use.

Avaya does not recommend customer to install the antivirus on Message Networking system (Linux based servers). Instead, Avaya recommends that the customer installs firewall on the network to protect the server. Message Networking does not perform any virus detection.

The customer must assume full risk for any undesired interactions between the anti-virus software and the Avaya product.

Anti-virus scanning may have great impact on the performance of the Avaya messaging servers prior to scanning for viruses. For example, performing a complete I/O file scan may have a negative impact on the relative server performance. Avaya recommends that you do not employ any message scanning that could drastically impact the performance of the Avaya servers.

Anti-virus programs are available in the form of standalone e-mail hosts, firewalls, and routers with embedded scanning.

General recommendations

The following are some general recommendations for limiting virus problems.

- Installs firewall on the network to protect the server.
- Never open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then double delete them by emptying your trash. Delete spam, chain, and other junk e-mail without forwarding it.
- Never download files from unknown or suspicious sources.

- Avoid direct disk sharing with read and write access unless there is a business requirement to do so.
- Always scan a diskette from an unknown source for viruses, before using it.
- Back up critical data and system configurations on a regular basis and store the data in a safe place.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Security policy



Security policy

A security policy is a statement of rules that must be followed by all the people who are given access to an organization's information and technology assets, both hardware and software. Security problems change constantly. Security measures that you implement today may not be so secure tomorrow. One of the most important tools for securing a system is to have a published security policy that you enforce. Having a security policy in place is of paramount importance for the functioning of your system in an efficient and secure manner and protecting the information assets of your organization. This security policy must include published security guidelines to inform users of their responsibilities; corporate policies defining network access, service access, local and remote user authentication, dial-in and dial-out, disk and data encryption, and virus protection measures; and employee training. All potential points of network attack must be protected with the same level of network security. In addition, the security policy must clearly:

- Identify what is to be protected.
- State what it needs to be protected against.
- State the possibilities and occurrences of well known threats.
- Describe processes to implement measures that protect corporate assets in a cost-effective manner.
- Describe processes for reviewing and improving the security measures on a continuous basis.
- Define corporate security goals.
- Include rules about negative or irresponsible behavior, a path of problem escalation, and information about who to notify of all security issues.
- Define measures that ensure that the security policy is not circumvented by anyone.

The security policy must be based on a carefully conducted security analysis, risk assessment, and business needs analysis. Refer to the Site Security Handbook memo (RFC2196) issued by the Internet Engineering Task Force at www.ietf.org for help on creating a security policy.

General security guidelines

Security is more than preventing hackers from eavesdropping on messages. It also means protecting your system against fraudulent long distance charges, corporate espionage, and malicious system intrusions. By recognizing the different types of hackers and the trails they leave, you can protect your system, and possibly catch the culprit. Prevention is your most effective weapon against voice mail hackers. In fact, almost all can be deterred with a combination of common-sense policies and procedures that involve better system design and administration, subscriber education, and effective company voice mail policies and guidelines.

A well established security policy can considerably enhance the security of your system. Following are some of the general guidelines that can help reduce unauthorized usage. Ensure that the security policy includes the following:

- **Protects System Administration Access.** Establish multiple access levels for subscribers, system managers, and system programmers. Require passwords for each level of access. Ensure that secure passwords exist for all logins that allow system administration or maintenance access to the system. Change the passwords frequently.
- **Provides Physical Security for Telecommunications Assets.** Locate your Message Networking system in a room with controlled access. Restrict unauthorized access to equipment rooms and wire connection closets. Protect system documentation and reports data from being compromised.

- **Monitors Traffic and System Activity for Abnormal Patterns.** Establish procedures and make review of system and network reports, to identify hackers, a weekly required part of system management. Activate features that turn off access in response to unauthorized access attempts. Use traffic and call detail reports to monitor call activity levels.

[Top of page](#)

Educate and train users

Everyone who uses the system is responsible for the security of the system. Informed people are more likely to cooperate with security measures that often make the system less flexible and more difficult to use. A bit of renewed awareness, perhaps in the form of a refresher course or an updated manual can go a long way in enhancing the general security of the system.

In addition, ensure that you do the following:

- Discourage the practice of writing down passwords. If a password needs to be written down, it must be kept in a secure place and never discarded while it is active.
- Establish well controlled procedures for resetting passwords.
- Establish procedures to counter social engineering. Social engineering is a con game that hackers frequently use to obtain information that may help them gain access to your system.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Security maintenance



Security maintenance

Through security maintenance, an organization can proactively manage the security of its systems. The importance of regular system maintenance should not be underestimated. Good, timely maintenance procedures can keep your systems running at optimum performance. Avaya recommends that you implement proper maintenance procedures in accordance with your corporate security policies and guidelines. See [system maintenance](#) for more information on Message Networking maintenance procedures.

Who is responsible?

You must define who is responsible for maintaining the security of your system. Security information must be distributed throughout the organization. It is the role of the information security department to communicate and validate that systems are being maintained. It is the role of the systems administrator to test and apply patches and maintain the security of the system.

If the security department is given the role of maintaining security, *and* validating and communicating security policy, then a conflict of interest would exist because the auditor and validator would also be the maintainer. Security staffs are often faced with limited personnel. It would be an impossible task for many security departments to take on the responsibility of maintaining system security throughout the enterprise. The task of maintenance needs to be distributed to all the system and application administrators. It is job of the security department to communicate and train the system administrators to secure systems according to the security policies, standards, and procedures of the organization.

Following are some of the general guidelines for defining a security maintenance program for your system:

Systems Backups

[Backups](#) are necessary to ensure that critical system data can be recovered in-case of an emergency or a system failure. As part of system maintenance activities, it is important that you do the following:

- Test system backup procedures at regular intervals.
- Test the system facilities to ensure that critical data can be fully recovered.
- Test the backup media to ensure that it can be restored.
- Test the restoration procedure regularly to ensure that the procedures are appropriate, restoration systems are adequate, and the restoration process can be completed within the time allotted in the recovery procedures.

Maintain and review activity logs and store them in a secure location. Activity logs can be used to trace system activity and errors.

Monitoring and alarming

System monitoring involves ongoing review of system reports and audits of the system and its logs. Review the security configuration on the system regularly to validate that changes made through maintenance do not weaken system security. It is also advisable to scan your system for vulnerabilities on a regular basis.

Message Networking supports a variety of security monitoring features. Web sessions are automatically disconnected after a period of inactivity. Accounts are automatically locked out for a period of time as a consequence of consecutive failed login attempts. All failed attempts to login are also logged for tracking user and administration activities. Security-related, critical events are reported in a maintenance alarm, which is

called out to an Avaya Maintenance Center through an analog telephone call. See [Overview of Message Networking logs](#) for more information on the logs generated by the system.

Security Audits

You can conduct a security audit of your system on a quarterly or an annual basis, as defined in your corporate security policies. Ensure that the security audit addresses the following components:

- Application security. A secure operating environment can be compromised by using an insecure application.
- Third-party application security. Ideally there should be no third-party applications running on the Message Networking system.
- Content. Review the security of the contents on the system. Often you need to address the security of items, such as passwords stored in HTML files.
- Network security. Review the security configuration of your network on a regular basis.

[Top of page](#)





Message Networking Help

[Home](#) | [Search](#) | [Print](#)
[Legal](#) | [Back](#) | [Fwd](#) | [Close](#)

[Getting Started](#)

[Administration](#)

[Installation](#)

[Maintenance](#)

[Reference](#)

[Home](#) > [Getting started](#) > [Concepts and features](#) > [System security](#) > Security references



Security references

Use the following references for more information on Security.

Avaya

Avaya Toll Fraud and Security Handbook

The Avaya Toll Fraud and Security Handbook provides important security information. You can check the [Avaya site](#) to get the latest copy of this handbook. You can also order by doing the following:

Call:

Avaya Publications Center

Voice: 1 800 457-1235, International Voice: 317 322 6416

Fax: 1 800 457-1764, International Fax: 317 322 6699

Write:

Avaya Publications Center

2855 N. Franklin Road

Indianapolis, IN 46219

Order

Document No. 555-025-600

Avaya Toll Fraud Crisis Intervention

If you suspect you are being victimized by toll fraud or theft of service and need technical support or assistance, call one of the following numbers immediately. These services are available 24 hours a day, 365 days a year. Consultation charges may apply.

- Technical Service Center's Toll Fraud Intervention Hotline at 1 800 643 2353
- Technical Services Organization Enterprise Customer number, 800 242 2121
- Technical Services Organization TCSS number, 800 225 7585

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or to securityalerts@avaya.com.

Information on Avaya Security Advisories and Notification is available at <http://support.avaya.com/security>

[Top of page](#)

