



Visual Modular Messaging Configuration Guide Release 2.1

16-300267
Issue 2.1
January 2005

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: <http://www.avaya.com/support>.

Trademarks

DEFINITY is a registered trademark of Avaya, Inc. MultiVantage is a trademark of Avaya, Inc. Windows, Windows 2000, and Windows NT are trademarks or registered trademarks of Microsoft Corporation.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

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

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: <http://www.avaya.com/support>. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

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

Your company's “telecommunications equipment” includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, “networked equipment”).

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

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

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

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

Responsibility for Your Company’s Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Standards Compliance

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

To order copies of this and other documents:

Call: Avaya Publications Center
 Voice 1.800.457.1235 or 1.207.866.6701
 FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
 200 Ward Hill Avenue
 Haverhill, MA 01835 USA
 Attention: Avaya Account Management

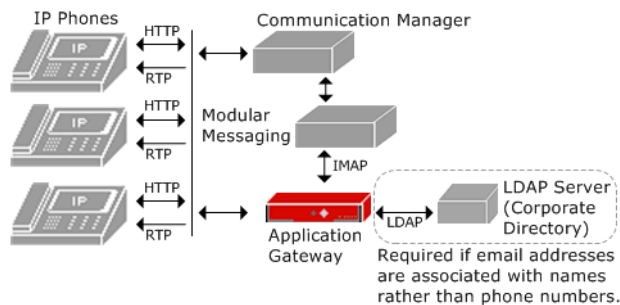
E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: <http://www.avaya.com/support>

Note Visual Modular Messaging will be available in a future release.

Avaya Visual Modular Messaging enables Avaya IP telephone (4620, 4620SW, 4610SW) users to review and manage voice mail from the telephone screen. Visual Modular Messaging displays messages that are managed by Avaya Modular Messaging (Release 2.0) and transcoded for display by the Avaya Phone Application Gateway (AG).

For Visual Modular Messaging operation, the AG connects to your network as follows:



The following topics describe how to configure the connection and operation of Visual Modular Messaging for Avaya IP phones:

- [Overview of Visual Modular Messaging, page 4](#)
- [Removing Visual Modular Messaging from the Voice Office Menu, page 4](#)
- [Configuring the Avaya File Server Script, page 5](#)
- [Verifying PBX Switch Configuration, page 5](#)
- [Configuring Visual Modular Messaging, page 5](#)
- [Adding Dialing Rules, page 9](#)

Note The AG distribution includes a document, *Using Visual Modular Messaging on Avaya IP Phones*, that you can change as needed and distribute to IP phone users. The document explains how to license and use the Visual Modular Messaging application.

Overview of Visual Modular Messaging

Visual Modular Messaging enables IP phone users to:

- Quickly scan a list of messages.
- View message details such as the caller name, the day/date/time and length of call, and the status of the message (played or not yet played).
- Listen to messages in any order. (Audio is converted to G.711 format.)
- Pause, fast forward, rewind, and delete messages.
- Call back the message sender without having to dial the number.

Visual Modular Messaging supports 24 concurrent audio streams. When an attempt to open a 25th audio stream occurs, the phone user will see an audio unavailable error message.

An IP phone user will be logged out of Visual Modular Messaging after an idle period configured in the Operation > Voice Office > Voice Mail page.

Removing Visual Modular Messaging from the Voice Office Menu

Note For more information on customizing the menus that display on IP phones, refer to the *IP Phone Menu Configuration Guide*.

If you do not want to give your IP phone users access to Visual Modular Messaging, remove it from the Voice Office menu as follows.

To remove Visual Modular Messaging from the Voice Office menu:

- 1 Open the Avaya AG Administration Tool: From a web browser, enter the URL **`https://AG_ipAddress:AG_adminPort`**.
- 2 Go to the **Operation > Voice Office > Menu** page.
- 3 Clear the checkbox for **Show Visual Modular Messaging**.
- 4 Click **Submit**.

Configuring the Avaya File Server Script

For information on configuring the Avaya file server script (**46xxsettings.txt**) so that phones can connect to the AG, refer to the guide *Configuring Avaya IP Phone Connections to the Phone Application Gateway*.

Verifying PBX Switch Configuration

PBX operation with Visual Modular Messaging requires that the following QSIG Optional Features are enabled through the switch's System Parameters Customer Options form. These are the recommended settings for switch operation.

- Basic Call Setup
- Basic Supplementary Services
- Supplementary Services with Rerouting
- Transfer into QSIG Voice Mail

Configuring Visual Modular Messaging

Note For information on configuring Avaya IP phones for operation with the AG, refer to the guide *Configuring Avaya IP Phone Connections to the Phone Application Gateway*.

To configure Visual Modular Messaging:

- 1 Open the Avaya AG Administration Tool: From a web browser, enter the URL **https://AG_ipAddress:AG_adminPort**.
- 2 Go to the **Operation > Voice Office > Voice Mail** page.

Network

Operation

Logging

Administration

General

Voice Office

Advanced

IP Phone

Menu

Directory

Voice Mail

Text Messaging

Visual Modular Messaging Guide

Unified Messaging Type

Avaya Modular Messaging

?

IMAP Server

IMAP Port

143

?

Alternate Address Server (LDAP)

☐

Session Configuration

Login Timeout (seconds)

1200

Submit

- 3 The Unified Messaging Type defaults to **Avaya Modular Messaging**.
- 4 Specify the IP address and the port of your Modular Messaging server.
- 5 If email addresses are associated with user name rather than phone number, you must specify the LDAP server to be used to look up the phone number. Select **Alternate Address Server (LDAP)** and fill in the fields as follows:

Field	Description
Server and Server Port	The IP address and port for your LDAP server.
	The LDAP Server Port defaults to 389. If you are using an indexed database, such as Microsoft Active Directory with a Global Catalog, changing the LDAP Server Port to 3268 will significantly speed the LDAP queries.
	Note If your directory is not indexed, we recommend that you use an administrative connection, rather than an anonymous connection, from the AG to the database. Download performance improves when you use an administrative connection.

Field	Description
Bind DN and Password	The Administrator Bind DN and password for queries to your LDAP directory. Examples of syntax for Bind DN: "ou=administrator,dc=ace,dc=com" and "cn=Administrator,cn=Users,dc=ace,dc=com" For Active Directory, the group name, specified as "cn=groupname", is required. For other LDAP directories, the group name either is not required or, if required, is specified as "ou=groupname". The AG binds to the LDAP server using the administrator credentials and then searches for the user. After locating the user, the AG unbinds the administrator credentials and rebinds with the user credentials. The password for the bind user is not needed if you connect anonymously.
Base DN	The Base DN, under which users are located, to be used as a starting point for Express Directory searches. Base DN is usually derived from the Bind DN by removing the user name and specifying the group where users are located. Example syntax for Base DN: "ou=Users,dc=ace,dc=com" and "cn=Users,dc=ace,dc=com"
Name	The common Name. Name defaults to "cn" and is typically set to "cn" or "displayName". This is the full name, such as Manuel Denz.
Surname	Another form of the name, comprised of the Surname (last name), followed by the delimiter ", " and the Given Name (first name). Defaults to "sn, givenName". For example, Denz, Manuel.
Given Name	Defaults to "givenName".
Email	Defaults to "mail".

Field	Description
Telephone Label and Field	The telephone number attribute defaults to "telephoneNumber". You can change this to any other attribute representing the phone number that you wish to display (such as "homePhone", "mobile", or "extension"). If your directory contains multiple entries for the chosen attribute, Visual Modular Messaging displays all of them. The label that you enter will display in Visual Modular Messaging. By default, the telephone number displayed is the full number, along with any prefixes configured, as described in “Adding Dialing Rules,” page 9. Note You must specify the phone prefixes so that returned calls to outside phone numbers are correctly dialed. For example, if a “9” is required to access an outside line and the long distance prefix is “1”, the phone prefix would be "9,1" or "9p1". (A comma “,”, p, or P provide a one-second pause.) For some sites the telephone numbers need to be customized, for example, to display only the last four digits. You can customize the telephone numbers, as described in “Adding Dialing Rules,” page 9.
Search Filter	The LDAP search filter to be used during a search. Defaults to "objectClass=*".
Search LDAP Directory by	The attributes to be used during a search. You can select one or more of the following attributes: Name (common name), Surname, and Given Name. (See the above note in “LDAP Search Filter” for information about searching by Given Name.)

- 6 Specify the Login Timeout value. This value determines how long a Visual Modular Messaging session can be idle before the user is logged out of the application.
- 7 Click **Submit**.

Adding Dialing Rules

By default, the full telephone number that is stored in a directory is dialed when the IP phone user selects a number in Visual Modular Messaging. You can customize telephone numbers as follows:

- You can specify the number of digits to be dialed. For example, you can specify that only the last four digits of numbers beginning with "423500" should be dialed. In that case, if the number in the directory is 423-500-0987, Visual Modular Messaging will dial 0987.
- You can specify the prefixes to be dialed with all numbers that are 3 to 5 digits, 6 to 7 digits, and 8 or more digits (as stored in the source directory).

Dialing rules apply to all configured directories.

To add dialing rules:

- 1 Go to the **Operation > Voice Office > IP Phone** page.

Visual Modular Messaging Guide

Dialing Rules

For numbers starting with: ...trim the number to last digits.

Example:
To dial only the last four digits for numbers such as 408-382-xxxx, specify **408382** and choose **4**. Use ? for wildcard.

Dial Prefixes to use for all numbers with:

3 to 5 digits

6 to 7 digits

8 or more digits **Example:** 91

Broadcast Server

Base URL **Example:** http://192.168.1.1/BCS

- 2 If your telephone system does not need to dial the full telephone number that is stored in a directory (perhaps for internal extensions), specify how the number should be trimmed.

For example, numbers that are internal to your telephone system might be stored in a directory as ten digits, yet only the last four digits should be dialed to reach an internal extension. Enter the unique starting numbers of those telephone numbers (such as the first six digits) and choose the number of digits to be dialed (such as the last four digits).

- 3 Specify the prefixes to be dialed for numbers, based on their length in the directory. Use a comma (,), "p", or "P" to insert a one-second pause. For example, "9,1" or "9P1".

You must specify prefixes so that returned calls to outside phone numbers are correctly dialed. For example, if a "9" is required to access an outside line and the long distance prefix is "1", the phone prefix would be "9,1" or "9p1".

- 4 Click **Submit**.