

MiCollab Advanced Messaging Web PhoneManager System Administrator Guide

For version 9.2 and above

Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2021, Mitel Networks Corporation

All rights reserved

Contents

Preface	5
References	5
Documentation	5
Documentation Updates	6
Help	6
Document Conventions	6
Frequently Used Terms	7
What is Web PhoneManager?	8
How it Works	10
Understanding Secure Sockets Layer (SSL) and Certificates	11
Acquiring a Certificate	12
Before Installing Web PhoneManager	13
Web Server Installation Requirements	13
Site Requirements	13
Microsoft Web Server Requirements	13
Microsoft Windows-based Apache Web Server Requirements	13
Linux-based Apache Web Server Requirements	14
Message Cache Manager Server Requirements	14
Workstation Installation Requirements	14
Installing Web PhoneManager	16
Configuring Web Server Software and Other Required Software	16
Configuring IIS	16
Configuring Apache Server	17
Installing the PHP Interpreter	18
Creating Working Folders in the PHP Directory	18
Editing the PHP.ini File (Linux)	18
Testing the PHP Interpreter	19
Changing the Permissions of the Configuration Directory	20
Configuring the Firewall	21
Installing Web PhoneManager	22

Configuring Web PhoneManager	23
Configuring Google reCAPTCHA™	23
Configuring Web PhoneManager Server Settings	23
Configuring Web PhoneManager Application Settings	27
Updating the Web PhoneManager Dashboard Tab	31
Updating the Administrator's Contact Information	33
Removing or Renaming the admin.php file for Added Security	35
Configuring Client Workstations	36
Installing Message Cache Manager	37
Configuring Message Cache Manager	38
Configuring Web PhoneManager for Message Cache Manager	40
Starting Message Cache Manager	41
Appendix A – Configuring Web PhoneManager with an XML or Text Editor	42
Appendix B – Configuring the User Resources Page with an XML or Text Editor	53
Appendix C – How to Upgrade Web PhoneManager	55
Appendix D – How to Configure Single Sign-On	56
Setting up ADFS 2.0 to Work with WPM SSO	56
Setting up MiCollab AM to Support SSO	57
Setting up WPM SSO to Work with ADFS 2.0	58

Preface

This guide describes how to install and configure Web PhoneManager™ and the Message Cache Manager.

This guide is written for Mitel-certified administrators and technicians who are familiar with MiCollab Advanced Messaging (MiCollab AM) procedures and terminology and the Microsoft Windows® operating system.

Before implementing any procedures in this guide, ensure that MiCollab AM software is installed and running successfully.

To successfully implement Web PhoneManager in an organization, the assistance of the following individuals, who constitute the implementation team, is required:

- MiCollab AM system administrator
- Microsoft Windows Server administrator
- Web server administrator
- MIS/IT support staff

IMPORTANT Ensure each member of the implementation team receives a copy of this administration guide several days or weeks before the implementation of Web PhoneManager.

References

A catalog of technical documentation is included on the MiCollab AM Installation Media. If you are installing any advanced applications, such as Networking and Fax Server applications, you should refer to the appropriate technical documentation for application and installation information.

Documentation

The technical documentation is produced in the PDF format and requires the PDF reader to view it. The MiCollab AM Documentation Library includes the following documents and resources:

- **Administration Documentation.** Available as a PDF only. Contains the following:
 - **Administration Guides.** Available as a PDF only. Contains administrative guides for administrators about how to manage and configure the messaging system.
 - **Quick Reference Cards (QRC).** Contains shortcuts and quick instructions telling subscribers how to access and use the messaging system.
 - **User Guides.** Available as a PDF only. Contains user guides for subscribers about accessing the messaging system and checking and sending messages.

- **Server Documentation.** Available as a PDF only. Contains the following:
 - **Developer Resources.** Contains programming guides and API references for developers for integrating the server clients and web applications with MiCollab AM.
 - **Installation and Configuration.** Available as a PDF only. Contains installation and configuration guides for server administrators about how to install and configure the messaging system.
 - **Integration Technical Notes (ITN).** Contains a set of guides that describe the integration methods and instructions for a variety of phone systems to work with MiCollab AM. The ITNs are generally used by resellers or administrators who are experienced with MiCollab AM and familiar with the integration procedures and terminology.
 - **Spare Parts Documentation.** Contains a set of guides that describe the instructions for installing and configuring hardware parts to work with MiCollab AM. These documents are written for Mitel-certified MiCollab AM technicians who are experienced with MiCollab AM and familiar with the procedures and terminology.
- **Software Release Notice (SRN).** This notice introduces the new features, capabilities, and hardware/software requirements for the corresponding MiCollab AM version.

Documentation Updates

Documentation updates may be available from the following sources:

- Mitel-certified technicians can view or download documents and program files from our partner web site: www.mitel.com

Help

The primary source of information about MiCollab AM is the online help available within any of its administrative utilities. You can access **Help** by clicking the **Help** button in the dialog box or window in which you are working.

Document Conventions

The following conventions are used in this document:

- **Key Names.** Names of keys on the keyboard are shown in a box.

Example: **Enter**

When two keys must be pressed simultaneously, they are joined by a + sign.

Example: **Alt** + **Tab**

- **Reference to Document** Titles of other documents are shown in italics.

Example: See the *System Installation and Configuration Guide*.

- **User Interface (UI) Element Names.** Names of UI elements such as dialog boxes, windows, screens, menu items, tabs, buttons, and icons are shown in bold.
| **Example:** On the **Startup** screen, click the **Start** icon.
- **User Input.** Information required to be typed is shown in italics.
| **Example:** Type the password *voicemail*.
- **Warning, Caution, Important, and Notes.** Text for the contents that require attention are shown as follows:

WARNING A warning paragraph advises you of circumstances that can result in the loss of data, harm to the MiCollab AM System Server platform, or personal harm.

CAUTION Failure to follow these recommendations can result in unauthorized access to the system and consequent loss of data.

IMPORTANT An important paragraph gives decision-making information or informs you of the order in which tasks need to be completed.

NOTE A note gives additional information, provides an explanation, or indicates an exception to the information in the preceding text.

Frequently Used Terms

Table 1. Frequently Used Terms

Terms	Description
System Server	<p>Term refers to an organization's computer platform(s) that have MiCollab AM software installed and handles the core system functions such as storing messages, database.</p> <p>It can also refer generically to the System Server platform, the Call Server platform, or both. The term is most often used to describe a software or hardware installation or configuration practice where the role of the server platform is not specifically expressed.</p>
Call Server	<p>Term refers to an organization's computer platforms that have MiCollab AM software installed and serve as the interface to the system (PBX). The Call Server(s) interface with the System Server for the purpose of accessing messages, and database.</p>

What is Web PhoneManager?

Web PhoneManager™ allows subscribers to manage their mailboxes and messages using the company's Intranet or an Internet connection through any supported Internet Web browser that has access to the server on which it resides.

Mitel has made every attempt possible to ensure that Web PhoneManager is compatible with browsers that support HTML 4.01, HTML 5.0, and standard JavaScript but results in such browsers may vary. Currently, Web PhoneManager supports the following web browsers:

- Apple Safari®
- Google Chrome
- Microsoft Edge
- Microsoft Internet Explorer® (Versions 9 and above)
- Mozilla Firefox®
- Opera

NOTE Refer to the current *Software Release Notice* for a list of supported browsers by operating system.

Web PhoneManager allows subscribers to manage their messages, their mailbox recordings, and their mailbox settings from an Internet browser software application.

Web PhoneManager provides a convenient menu pane and a system of tabs that organizes messages and mailbox settings that allows subscribers quick and easy access to their mailbox. Subscribers with questions about Web PhoneManager, or about MiCollab AM in general can click the **Help** button to launch a browser-based help system in a new browser window. In addition, subscribers can click the **User Resources** link on the navigation bar for additional user guides (as shown in [Figure 1](#)).

NOTE Certain portions of Web Phone Manager, such as the **Availability Settings**, **VIM**, **SMS**, **Notification**, and **Forwarding** tabs, are available only if the MiCollab AM system is licensed and configured to use the feature, and the administrator has configured those features for the particular Subscriber mailbox. Note also that access to Web PhoneManager from outside the organization's intranet depends on the web server's accessibility from outside the company firewall.

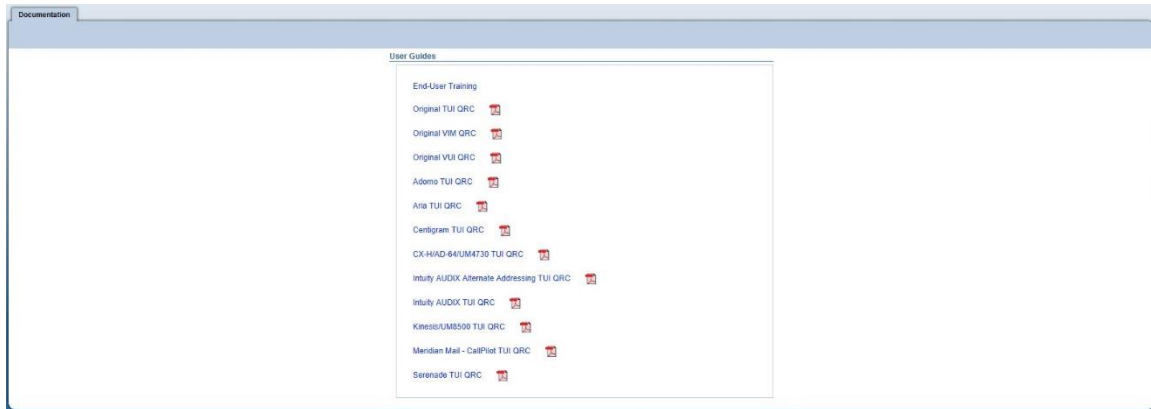


Figure 1. Web PhoneManager User Resources link

If Web PhoneManager message access is enabled in a subscriber's mailbox, the subscriber sees the **Inbox** tab immediately after logging on to Web PhoneManager. On this tab ([Figure 2. Web PhoneManager – Inbox tab](#)), the subscriber can perform the following tasks:

- Send voice messages
- Listen to voice messages, reply to them, and forward them
- View fax messages, reply to them, and forward them (if XMediusFAX or RightFax is integrated with the MiCollab AM system)
- View, save or delete voice and fax messages

Adjacent to the **Inbox** tab, the **Saved** and **Trash** tabs allow the subscriber to review saved messages and recover messages awaiting deletion.

Depending on the organization's security needs, the administrator can allow the subscribers to select one or more of the following methods for listening to voice messages:

- **Telephone playback** requires a MiCollab AM subscriber to configure Web PhoneManager with a telephone number that MiCollab AM can reach by dialing. When the subscriber selects a message and clicks the Play button, MiCollab AM dials the specified telephone. The subscriber answers and listens to the message.
- **Streaming playback** delivers the voice message as a compressed MP3 audio file to an embedded multimedia playback. When the user clicks the **Play** button, MiCollab AM compresses the voice message and sends it to the embedded player in the user's web browser. The browser then plays the message through the user's computer.
- **Download and playback** allows the subscriber's workstation to create a temporary copy of the message after the subscriber clicks the Play button. The subscribers preferred media player then opens the temporary copy and plays it.

NOTE Recording new messages, greetings, and announcements must occur over a telephone that is accessible to MiCollab AM. Playback of existing greetings (unlike messages) requires telephone playback regardless of the message playback type selected.

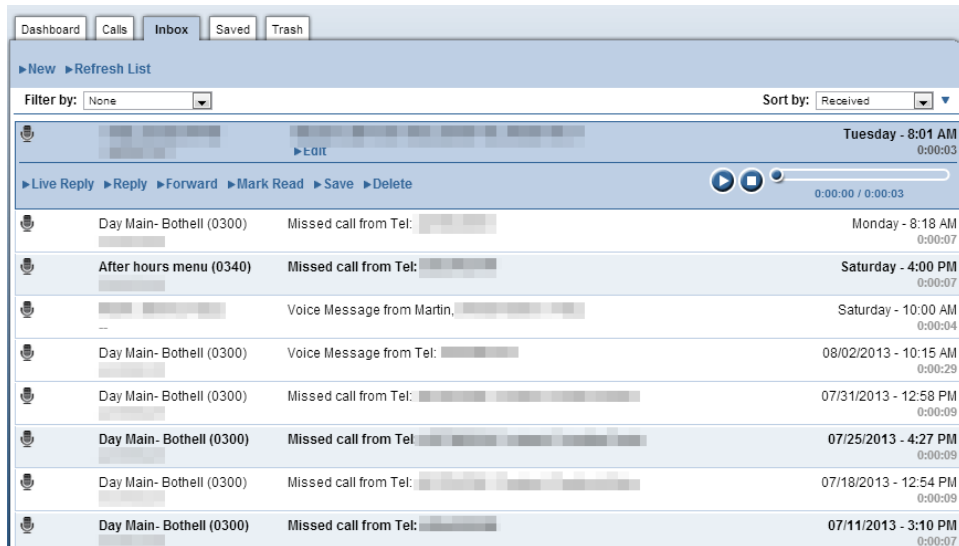


Figure 2. Web PhoneManager – Inbox tab

How it Works

Web PhoneManager operates as a PHP web server application. It acts as a liaison between the client workstation and the MiCollab AM System Server. When a subscriber logs on to Web PhoneManager, a connection is established with the System Server. The Subscriber mailbox information is sent to the client workstation, and a subscriber session is initiated. For security purposes, Web PhoneManager enables you to encrypt these transactions using Secure Sockets Layer (SSL) on the web server.

MiCollab AM Mobile for Web offers a subset of Web PhoneManager functions optimized for web browsers in mobile phones. MiCollab AM Mobile for Web installs automatically with Web PhoneManager. If Web PhoneManager is installed, open the root URL for Web PhoneManager server and append **/mobile** to access the mobile phone browser optimized site.

For example:

If Web PhoneManager is installed as **http://wpm.mycompany.com**,
use **http://wpm.mycompany.com/mobile** to access MiCollab AM Mobile for Web.

Message Cache Manager is a multi-purpose program that communicates with the Web PhoneManager server and the System Server. It is a transparent application that acts as a liaison between the Web PhoneManager application and the MiCollab AM System Server. It provides the following features to the Web PhoneManager and MiCollab AM environment.

- Reduces the performance load of the System Server
- Optimizes SOAP System Server requests from Web PhoneManager for message information
- Supports multiple Web PhoneManager servers
- Supports multiple System Servers (Digital Networking)
- Multiple Message Cache Manager applications can point to one System Server

NOTE Web PhoneManager depends on the Message Cache Manager to get messages for logged on users. For a single tenanted or multi-tenanted system, the MiCollab AM system SOAP server acts as a Message Cache Manager, and therefore a separate standalone Message Cache Manager is recommended, but not required, for Web PhoneManager.

IMPORTANT If using the *Availability* feature, be sure to synchronize the Web Server's clock with the System Server in order for the *Availability* automation to stay precise and perform accurate time calculation.

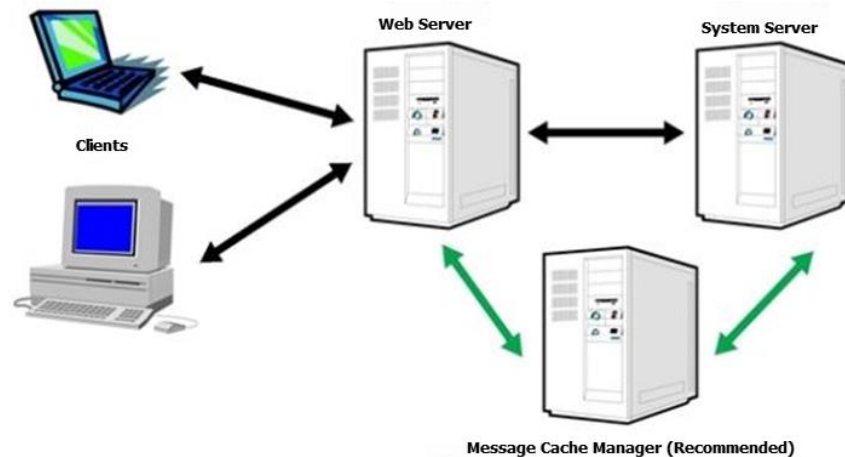


Figure 3. Web PhoneManager, MiCollab AM, and Message Cache Manager (Recommended)

Understanding Secure Sockets Layer (SSL) and Certificates

Most common web servers support a standard protocol for providing data security layered between the service protocols HTTP and TCP/IP. This security protocol, called Secure Sockets Layer (SSL), provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. The HTTPS protocol allows access to a web page secured by SSL.

SSL provides a security *handshake* that is used to initiate the TCP/IP connection. This handshake results in the client and server agreeing on the level of security they use and fulfills any authentication requirements for the connection. Thereafter, SSL's only role is to encrypt and decrypt the bit stream of the application protocol. The information in both the HTTPS request and the HTTPS response is encrypted, and includes:

- The Uniform Resource Locator (URL) the client is requesting
- Any submitted form contents
- Any HTTPS access authorization information (user names and passwords)
- All of the data returned from the server to the client.

To complete the handshake, the web server must have a certificate installed.

IMPORTANT Web PhoneManager does not include a certificate. You must purchase and install a certificate to use SSL.

Acquiring a Certificate

To use SSL, a certificate must be purchased from (and renewed annually by) a Certificate Authority (CA), which issues digital certificates and validates the holder's identity and authority. A CA embeds an individual's or an organization's public key along with other identifying information into each digital certificate and then cryptographically *signs* it as a tamper-proof seal, verifying the integrity of the data within the certificate and validating its use.

You can purchase certificates from a CA such as the following:

- VeriSign® Inc.
- Thawte® Digital Certificate Services

For instructions on acquiring and installing a certificate on your web server platform, refer to the following locations on the World Wide Web:

- For instructions on installing certificates under Microsoft Internet Information Services (IIS), refer to the following Microsoft Knowledge Base article at support.microsoft.com/kb/816794.
- For instructions on configuring the Apache Web Server 2.2 SSL module for Linux, refer to httpd.apache.org/docs/2.2/ssl.
- For instructions on installing and configuring the Open SSL toolkit, on which the Apache SSL module depends, refer to www.openssl.org/docs.

Before Installing Web PhoneManager

This section lists the installation requirements for successfully installing Web PhoneManager. Be sure to review and meet these requirements before continuing with the other procedures discussed in this document.

Web Server Installation Requirements

Be sure to review the following installation requirements to ensure that the correct files, versions, and Service Packs are installed on your web server.

NOTE Web PhoneManager version 9.0 requires MiCollab AM version 9.0.

Site Requirements

- TCP/IP-based connectivity between the web server and the MiCollab AM server
- TCP/IP network connectivity with the Message Cache Manager server (if deployed)
- Web PhoneManager and Message Cache Manager may run on the same physical platform or as VMware® virtual machines running on the same platform

Microsoft Web Server Requirements

- Windows Server 2012 R2, Windows Server 2016 (Server with Desktop Experience), or Windows Server 2019 (Server with Desktop Experience) with the Windows Internet Information Server (IIS) version 6.x, 7.0, 7.5, 8.x, or 10.x component installed
- World Wide Web Publishing Service installed and running
- PHP version 7.4.1 with SOAP, XSL, and OpenSSL modules installed
- To ensure web security using SSL, a certificate purchased from a Certificate Authority
- Access to a DVD/USB drive (for software installation)

Microsoft Windows-based Apache Web Server Requirements

- Windows Server 2012 R2, Windows Server 2016 (Server with Desktop Experience), or Windows Server 2019 (Server with Desktop Experience)
- Apache Web Server versions 2.2.x or above
- PHP version 7.4.1 with SOAP, XSL, and OpenSSL modules installed
- To ensure web security using SSL, a certificate purchased from a Certificate Authority

- Access to a DVD/USB drive (for software installation)

Linux-based Apache Web Server Requirements

IMPORTANT Most current Linux server distributions include copies of Apache and PHP. However, because those distributions are not updated between releases, you may need to download, build, and install the required versions of Apache and PHP.

- Current server-class Linux distribution such as Fedora®, Debian®, or OpenSUSE® Linux
- Apache Web Server versions 2.2.x or above
- PHP version 7.4.1 with SOAP, XSL, and OpenSSL modules installed
- OpenSSL
- To ensure web security using SSL, a certificate purchased from a Certificate Authority
- Access to a DVD/USB drive (for software installation)

Message Cache Manager Server Requirements

- Windows Server 2012 R2, Windows Server 2016 (Server with Desktop Experience), or Windows Server 2019 (Server with Desktop Experience)
- TCP/IP networking
- The firewall on the Message Cache Manager Server platform must have TCP port 18276 for unencrypted communication and port 18277 for SSL communication open so that Web Phone Manager can access the Message Cache Manager Server.
- Message Cache Manager can run on the same server platform as Web PhoneManager, as a separate VMware virtual machine, on a separate stand-alone server, or on a shared server with available processing capacity.

Workstation Installation Requirements

Workstations must have access to the following software and capabilities to use Web PhoneManager. For more information, refer to the [Configuring Client Workstations](#) section. The following are the minimum requirements for client workstations running Web PhoneManager:

- Compatible web browser (refer to the [What is Web PhoneManager?](#) section)
- Connection to the local area network (LAN) or to the World Wide Web via an Internet Service Provider (ISP)
- (optional) To view fax messages, a fax viewer capable of displaying multiple-page TIFF documents, such as the XMediusFAX Viewer, the Microsoft Windows Picture and Fax Viewer, or Apple Preview for the Macintosh.

NOTE To find a multiple-page TIFF viewer for a Linux-based workstation, consult the software package repository for the Linux distribution installed on the workstation.

- The ability to record or review voice messages and greetings requires a telephone. Subscribers can use the telephone to review and record these recordings.

IMPORTANT Subscribers who reach Web PhoneManager through a dial-up Internet account must have a separate telephone line in order to use the **Reply** and **Live Reply** features. That line must be able to receive incoming calls, and its telephone number must be accessible through the Call Server's dialing plan. Subscribers with dial-up internet accounts can, however, use the Download or stream playback features.

Installing Web PhoneManager

Regardless of which server platform you choose to host Web PhoneManager – IIS on Windows, Apache on Windows, or Apache on Linux – the basic stages of installation are as follows:

- Install or update the web server software.
- Install the PHP interpreter with its SOAP, XSL, and OpenSSL modules.
- Install and configure the Web PhoneManager software.

This section discusses these stages in more detail.

Configuring Web Server Software and Other Required Software

Because of the variety of different web server platforms, this document assumes that you have the web server and all associated software installed and running. If the web server software is not installed, please refer to the documentation appropriate to your operating system and web server selection.

In addition to the web server software, for all web server platforms, install PHP. You can download the software at www.php.net. Follow the installation instructions appropriate to your operating system and web server combination. For Web PhoneManager specific configuration instructions, refer to the [Installing the PHP Interpreter](#) section.

NOTE PHP.net does not offer .msi installers for windows for PHP 7.4.1. Microsoft Web Platform Installer 5.1 does offer PHP installations.

Configuring IIS

Before you configure IIS, add a folder to the **\inetpub\wwwroot** folder on your web server. Name the new folder wpm. It becomes the root folder for the Web PhoneManager website.

While you are configuring IIS, do the following:

- If you are deploying more than one site, each one must have its own unique port. The customary default port for websites is 80, but adjacent port numbers such as 75 or 82 also work.
- In the list of starting page names for the default website, add **index.php** and move it to the top. This frees subscribers from typing the file name of the page as part of the Web PhoneManager web address (URL).
- After you have set up IIS, create a new website using the **\inetpub\wwwroot\wpm** folder as the home directory.

- You may also want to create a test website and populate it with static HTML pages. Using a browser on a second computer, log on to the test site and make sure it functions normally. This tests IIS itself and verifies that the basic IIS installation is working correctly.
- After you have finished configuring IIS, stop all websites except for the default site.

Configuring Apache Server

After you have installed the Apache software, you need to adjust a few of its default settings so that it runs correctly. These settings are located in a configuration-setting file named **httpd.conf**.

IMPORTANT The following procedure discusses only the configuration settings that pertain directly to Web PhoneManager. Changing other configuration settings can prevent your Apache server from operating correctly. For more information about Apache configuration, refer to <httpd.apache.org/docs/2.2/configuring.html>.

To configure your Apache server:

- 1 From the Start menu, go to **All Programs > Apache HTTP Server > Configure Apache Server**, and then click **Edit the Apache httpd.conf Configuration File**.
- 2 In the configuration file, update the following settings to the values shown.

Table 2. Apache Server Configuration Values

Setting	Value	Comment
DocumentRoot	<apachefolder>/htdocs	In most circumstances, you can leave this at its default, which is based on the directory where you installed the Apache software (shown here by <apachefolder>).
DirectoryIndex	index.php index.html	

- 3 From the menu bar, go to **File > Save**, and then click **Exit**.

NOTE It is recommended that you restart the web server platform after the installation and configuration of the Apache server is complete.

The Apache Web Server software installation places a test page in the server's document root directory. To display the test page, start a web browser on another computer within the web server's network and navigate to **http://myserver**, where **myserver** is the full address you have assigned to the server. You should see the words **It works!** in the browser.

Installing the PHP Interpreter

Because of differences in server platform, web server, and web server configuration, instructions on how to install and configure PHP is beyond the scope of this document.

Consult the documentation for your operating system and web server for detailed instructions. Once the PHP interpreter is installed and configured, there are several things to do to allow the installation to work with Web PhoneManager.

NOTE PHP is available as two different Windows installers. One is the Thread Safe installer. The other is the Non-Thread Safe installer. The Non-Thread Safe version uses FastCGI and is recommended for IIS 7.0 and up.

Refer to php.net/manual/en/install.windows.iis7.php for instructions on installing PHP on Microsoft IIS 7.0 and later. For general Windows installation instructions, please refer to php.net/manual/en/install.windows.php.

Creating Working Folders in the PHP Directory

After you have installed the PHP software, create two new folders named **Upload** and **Session** within the directory where you installed PHP. During Web PhoneManager sessions, PHP uses these folders as temporary holding locations for uploaded files and session information.

To ensure that these folders function properly for all MiCollab AM subscribers, check and adjust their access permissions as shown in the following table.

Table 3. PHP Directory Folder Directions

If your web server runs...	Then...
Windows	The web service account must have write permissions to these folders/directories.
Linux	Use the chmod and chown commands to give the default web user account ownership and read, write, and file execute (but not directory execute) privileges for the folders.

Editing the PHP.ini File (Linux)

After you have installed PHP and its SOAP, OpenSSL and XSL modules, use a text editor to open the **PHP.ini** file. This file is located in the root directory that you specified for PHP during its installation.

NOTE You do not need to edit the **PHP.ini** file on a Windows Server 2012 R2, Windows Server 2016 (Server with Desktop Experience), or Windows Server 2019 (Server with Desktop Experience) platform. Under Linux, editing of the PHP.ini file varies with each distribution and build. You can still update the PHP.ini file to pick the location of the session and upload folders for logging. Currently, it sets this path for logging: C:\Windows\temp.

In the **PHP.ini** file, verify that the settings in the following table are assigned the values shown. If not, change the settings as needed.

Table 4. PHP.ini File Settings

Setting	Location	Value
cgi.force_redirect	Paths and Directories	0 (if PHP is running in CGI mode)
upload_tmp_dir	Fopen wrappers	The full path to the Upload folder in the PHP root directory
session.save_path	Fopen wrappers	The full path to the Session folder in the PHP root directory

Verify that references to the SOAP, OpenSSL, and XSL modules are added. These references have the following general format:

Extension = filename

Where **filename** refers to the actual filename of the module. (The filename can vary between Windows and various Linux distributions.)

Table 5. Module References

If your web server runs...	Then you can find the module references...
Windows	In sections named [PHP_SOAP] and [PHP_XSL] at the end of the php.ini file
Linux	In separate files called soap.ini and xsl.ini, which may be located in an alternate configuration directory (see the PHP status page in the following procedure for the name of this directory if necessary)

Testing the PHP Interpreter

Once you have installed the PHP interpreter, you can use the web server to test it. The following procedure explains how to call up the PHP status page in a web browser.

IMPORTANT Mitel Technical Support personnel cannot help you troubleshoot your installation of Web PhoneManager until your web server has passed this test.

To test the PHP interpreter:

- 1 Start a text editor on your web server platform, and then create a new document.
- 2 In the new document, type the following text: `<?php phpinfo(); ?>`
- 3 Save the new document in the default root folder of your web server as a text file named **phptest.php**.
- 4 At a different computer that has network access to the web server, start a web browser. On the browser's address line, enter the address:
http://servername/phptest.php
Where **servername** is the network name or domain name of your web server
- 5 Proceed according to the result you see in your web browser.

Table 6. Web Browser Possible Outcomes

If you see...	Then...
An error page	Examine your web server software and reconfigure it as needed.
The PHP status page	Continue to next step.

- 6 Scroll down the PHP status page to verify that the SOAP, OpenSSL, and XSL modules are installed and enabled.

Table 7. Modules Possible Outcomes

If...	Then...
One or more modules are not installed or enabled	The PHP interpreter is not configured correctly. Examine your installation of PHP and reconfigure it as needed.
All modules are installed and enabled	The web server and PHP interpreter are working correctly. Continue to next step.

- 7 Exit your web browser.

Changing the Permissions of the Configuration Directory

Upon initial configuration of your Web Phone Manager system, you must make the config directory on your web server writable to the web server's guest account. As such, you need to update the permissions

of the config folder to give full control to the either the Internet Guest Account (if you are using IIS) or to the default web user (if you are using the Apache web server).

To ensure that the directories and files in the Web PhoneManager site are available to MiCollab AM subscribers, check and adjust the folders access permissions as shown in the following table.

Table 8. Web Server Access Permissions

If your web server runs...	Then...
Windows 2016/2019 IIS 10.x	Grant Full Control permissions to the default Internet Guest Account on the web server platform (USER_platformname)(IIS8.5 account is IUSR)
Windows 2012 R2 IIS 8.x	Grant Full Control permissions to the default Internet Guest Account on the web server platform (USER_platformname)(IIS8.5 account is IUSR)
Linux	Use the chmod and chown commands to give the default web user account ownership and read, write, and file execute (but not directory execute) privileges for the folders.

Configuring the Firewall

If your organization maintains a firewall between its web-based servers and the organization's users, you must open the port addresses in the following table for Web PhoneManager to function correctly.

Table 9. Port Configuration Purposes

Port	Purpose
80	Primary HTTP port for the Web PhoneManager site
NOTE If you specified a different HTTP port when you installed the web server, substitute port 80 with the port number you specified.	
443	Secure HTTP (HTTPS) port
18277	Secure SOAP port

IMPORTANT If you are installing Web PhoneManager on an IIS server, you must go back to IIS Administration and start the Web PhoneManager website now.

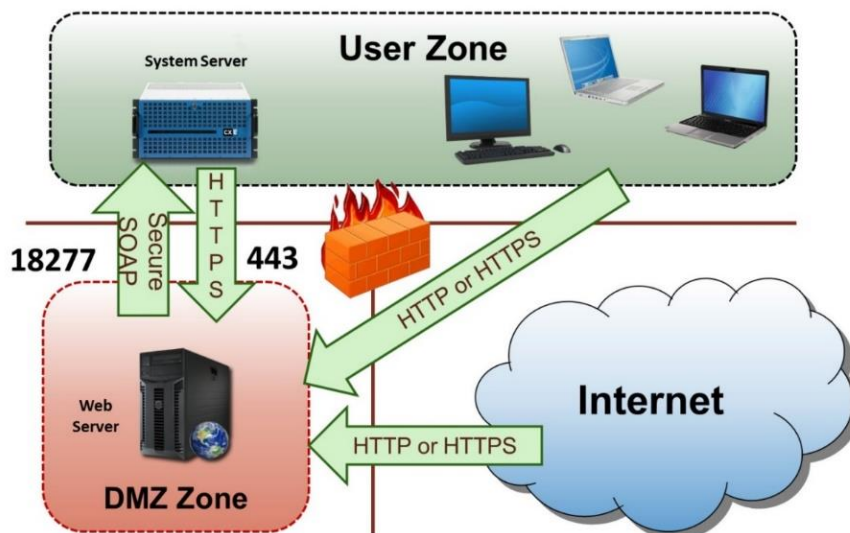


Figure 4. Firewall Setup Diagram

Installing Web PhoneManager

Because Mitel has designed Web PhoneManager to run on two different web server platforms and two different operating systems, Web PhoneManager is supplied on the MiCollab AM Installation Media without a specific installation program. Instead, the files and directories that make up Web PhoneManager are included on the installation media exactly as they must be installed on a web server.

To install Web PhoneManager on the web server platform:

- 1 Log on to the platform using a Windows Administrator account.
- 2 Insert the MiCollab AM Installation Media into the appropriate drive.
- 3 Do one of the following:

Table 10. Autorun Options

If autorun is...	Then...
Enabled	The MiCollab AM Installation Media menu appears. In the MiCollab AM Server Components area, click Browse this disc, and then open the Web Applications folder on the media.
Not Enabled	Open the Web Applications folder on the media, and then continue to next step.

IMPORTANT In the following step, be sure to preserve and restore the original directory structure stored in the **\Web Applications\wpm** folder on the installation media.

- 4 Copy the contents of the **\Web Applications\wpm** folder, including all subfolders, to the Web PhoneManager site directory on the web server.

Configuring Web PhoneManager

Once you have installed the Web PhoneManager software, you must designate the network location of the MiCollab AM System Server. The following procedure describes how to make these modifications and configure the basic Web PhoneManager settings.

NOTE For additional configuration options, see [Appendix A – Configuring Web PhoneManager with an XML or Text Editor](#).

Configuring Google reCAPTCHA™

Administrators can enable a Google reCAPTCHA human verification response test to display on the Web PhoneManager logon page, the Security Request page, or both. Before configuring Web PhoneManager to use reCAPTCHA, it is important to understand what reCAPTCHA is and what it does. The reCAPTCHA system uses advanced risk analysis techniques to help a web page distinguish between legitimate users and potentially abusive bots. Users are required to select the *I'm not a robot* check box (and in some cases, validate whether or not they are human by selecting images) to continue.

You will need a private and public key to configure the reCAPTCHA portion of the Web PhoneManager. The private and public keys are generated from the Google reCAPTCHA administrator website. For more information, or to obtain free reCAPTCHA keys for your website, visit <https://www.google.com/recaptcha/intro/>.

Configuring Web PhoneManager Server Settings

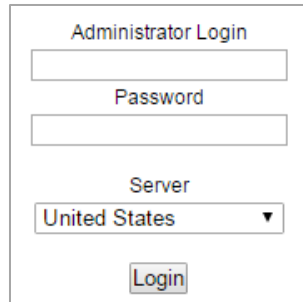
To configure Web PhoneManager Server Settings:

- 1 Launch your web browser and access the **admin.php** file for Web PhoneManager by typing the following into the address field on your web browser:

http://servername/admin.php

Where **servername** is the network name or domain name of your web server.

The **Administrator Login** page for your Web PhoneManager web server appears.

A screenshot of a web form titled "Administrator Login". It contains three input fields: a text box for the username, a text box for the password, and a dropdown menu for the server. The dropdown menu is currently set to "United States". Below these fields is a "Login" button.

Administrator Login

Password

Server

United States ▼

Login

- 2 Type your MiCollab AM **Administrator Login** Username and **Password**, select the **Server** from the drop-down list, and then click **Login**. The **Web PhoneManager Settings** page appears.

NOTE The default **Administrator Login** Username is *administrator* with the **Password** field left blank.

Web PhoneManager Settings

Application Settings

Interface

Default Language: en

☒ Use Javascript/AJAX Interface

☒ Allow Full Directory Listing

☒ Allow users to edit Personal Operator field

☐ Allow users to set devices as trusted

Playback Speed settings available: Message, Session

Message Access

☒ Telephone

☒ Streaming Media (requires Flash plugin)

☒ Download

Default Playback Type: Streaming Media

Message List

☐ Purge Deleted Messages On Exit

☒ Allow Message List Refresh

Message List Refresh Time (minutes): 5

Authentication

☐ Enable Secure Cookie Flag

☒ Allow Remember Me

Days to Remember Me: 2

☒ Show Security Code Reset Link

☐ Enable reCAPTCHA for security reset request page

☐ Enable reCAPTCHA for login page

reCAPTCHA API Public Key:

reCAPTCHA API Private Key:

Expose Availability Settings to Subscribers

☒ Enable Availability Processing setting

☒ Announce Availability settings

☒ Find-me Devices settings

☒ Allow Call Alert notification for mobile client devices

☒ Enable Call Screening

☒ Route to Subscriber settings

☒ Message Acceptance setting

☒ Device Types

SAML SSO

IdP Metadata URL:

[Fetch IdP Information](#)

IdP Information

IdP Target URL:

IdP Certificate:

Assertion URL:

Application Identifier:

WebServices UserID:

WebServices Password:

CX Servers

Encryption Type: None

	Server Display Name	Server Address	Tenant Name	
1	<input type="text" value="ServerName1"/>	<input type="text" value="TenantServer1"/>	<input type="text" value="Tenant1"/>	Remove 1
2	<input type="text" value="ServerName2"/>	<input type="text" value="TenantServer2"/>	<input type="text" value="Tenant2"/>	Remove 2
	<input type="text"/>	<input type="text"/>	<input type="text"/>	Add New

Message Cache Manager Address:

- In the **MiCollab AM Servers** group, select the **Encryption Type** from the drop-down menu. Select **None** if you do not want to use encryption. Select **SSL** to enable encryption. The default is **SSL**.
- Enter a name in the **Server Display Name** field. This displays the name of your MiCollab AM System Server.
- In the **Server Address** field, enter the **IP Address** or **Fully Qualified Domain Name (FQDN)** of your MiCollab AM System Server.
- In the **Tenant Name** field, enter the name of the tenant.
- In the **Message Cache Manager Address** field, enter the IP address or the FQDN of the Message Cache Manager server.
- Click **OK** to update the configuration.

NOTE If you see a message like **Missing mandatory configuration element <soap_protocol>**, you need to run the Administration tool again and click the **OK** button to save the configuration.

The following table describes each setting in more detail.

Table 11. Web PhoneManager Settings – MiCollab AM Servers Descriptions

Web PhoneManager Settings – MiCollab AM Servers Descriptions	
MiCollab AM Servers	Description
Encryption Type	<p>Select the type of encryption to use by Web PhoneManager when communicating with the System Server and Message Cache Manager.</p> <p>Select None if you do not want to use encryption. Select SSL to enable encryption. The default is SSL.</p> <p>IMPORTANT Failing to set the encryption type explicitly on the configuration page can cause connections to fail after an upgrade.</p>
Server Display Name	Displays the name of your MiCollab AM System Server.
Server Address	Displays the IP address or FQDN of your MiCollab AM System Server.
Tenant Name	Enter the name of the tenant.
Add New	<p>Click Add to insert a new row, and then add a new MiCollab AM System Server.</p> <p>NOTE If you are using Web PhoneManager to access multiple MiCollab AM System Servers, you must identify all System Server addresses in the Server Display Name and Server Address fields.</p>
Remove	Click Remove to remove the corresponding MiCollab AM System Server.
Message Cache Manager Address	Enter the IP address or the FQDN of the Message Cache Manager server.

Configuring Web PhoneManager Application Settings

The **Web PhoneManager Settings** page contains Application Settings that can be configured according to the guidelines provided in the following table:

Table 12. Web PhoneManager Settings – Application Settings

Web PhoneManager Settings – Application Settings	
Interface	Description
Default Language	Click the drop-down box to display the list of languages, and then select the default language that you want to display on your Web PhoneManager web pages. The default is en (English).
Use JavaScript/AJAX Interface	Select to enable or clear to disable the AJAX (asynchronous Java Script and XML) interface. The default is enabled. NOTE It is recommended that you keep the Java script/AJAX interface enabled. Disabling the Java script/AJAX interface disables features in Web PhoneManager.
Allow Full Directory Listing	Select to enable or clear to disable the listing of the full user directory for your organization. The default is enabled. NOTE If your directory is very large, it is recommended that you disable the Full Directory Listing to prevent PHP time-outs.
Allow users to edit Personal Operator field	Select to enable or clear to disable the users' ability in Web PhoneManager to edit the Personal Operator field. The default is enabled.
Allow users to set devices as trusted	Select to enable or clear to disable the users' ability in Web PhoneManager to set a device as trusted or auto logon. The device must be associated with the user's Subscriber mailbox for the Trusted attribute to be enabled. The default is disabled. IMPORTANT The MiCollab AM administrator must configure MiCollab AM to allow trusted logons before subscribers can configure a device as trusted. For more information, refer to the MiCollab AM help topic <i>Allowing Trusted Logons</i> . NOTE When a device is set as trusted or auto logon, a call made directly from the device number to MiCollab AM

automatically logs the subscriber on to their MiCollab AM mailbox, thereby skipping the entry of the security code.

Playback Speed settings available	Select if subscribers can use the playback speed mechanism during a Message Session or not (none). The default is Message, Session .
-----------------------------------	---

Message Access	Description
Telephone	Select to enable or clear to disable the user's ability in Web PhoneManager to listen to messages through the telephone. The default is enabled.
Streaming Media (requires plugin)	<p>Select to enable or clear to disable steaming playback of messages. Streaming playback delivers the voice message as a compressed MP3 audio.</p> <p>When the user clicks the Play button, MiCollab AM compresses the voice message and sends it to the embedded player in the user's web browser, which then plays the message through the user's computer. The default is enabled.</p>
Download	Select to enable or clear to disable the ability to create a temporary copy of the message on the subscriber's workstation after the subscriber clicks the Play button, or to save a copy of the message to their hard drive. The default is enabled.
Default Playback Type	Select the default message playback type for Web PhoneManager from the list. The options include Streaming Media, Telephone , or Download . The default is Streaming Media .

Message List	Description
Purge Deleted Messages On Exit	<p>Select to enable or clear to disable the purging of deleted messages when a user exits Web PhoneManager. The default is disabled.</p> <p>NOTE If enabled, a subscriber's trash folder is emptied at the end of their current session.</p> <p>If disabled, messages remain in the trash folder until the subscriber empties their trash or the system removes the trash messages automatically based on the message retention settings of the Subscriber mailbox.</p>
Allow Message List Refresh	Select to enable or clear to disable the Message List Refresh option. The Message List Refresh parameter refreshes the

message list in Web PhoneManager at the frequency you set in the **Message List Refresh Time minutes** field. The default is enabled.

Message List Refresh Time (minutes)	Specify the amount of time (in minutes) that passes before Web PhoneManager automatically refreshes a user's message list. The default is five minutes.
Authentication	Description
Enable Secure Cookie Flag	<p>Select to enable or clear to disable the cookie for SSL (HTTPS). When enabled the subscriber's browser can only send a cookie to Web Phone Manager using SSL (Secure Socket Layer). This setting is enabled by default.</p> <p>NOTE If the Web PhoneManager site is not using SSL or HTTPS, do not enable the Secure Cookie Flag. Subscribers are unable to access Web PhoneManager if this flag is enabled and you are not using SSL.</p>
Allow Remember Me	<p>Select to enable or clear to disable the web browser's ability to remember a Web PhoneManager user's login information. The default is enabled.</p> <p>If enabled, this appears in the form of a Remember me on this computer checkbox on the login page. If disabled, the checkbox does not appear on the login page.</p>
Days to Remember Me	<p>Specify the number of days that a subscriber's login information persists if the Allow Remember Me option is enabled. When subscribers reach the end of their allotted login save days, they can re-select the Remember me on this computer check box to re-start their allotted number of login save days. The default is 2 days.</p>
Show Security Code Reset Link	<p>Select to enable or clear to disable the Security Code Reset Link (Forgot Security Code?) on the subscriber logon page and on the Security Code tab of the Personal Settings page. This setting is enabled by default.</p> <p>NOTE For information on using and configuring the Security Code Reset feature, please see the following topic in the MiCollab AM online help: <i>Configuring the Security Code Reset Feature</i>. In addition, for this feature to work properly, the default SMTP provider in MiCollab AM must be properly configured. Please refer to MiCollab AM documentation for configuration instructions.</p>

Enable reCAPTCHA for security reset request page	Select to enable the reCAPTCHA human verification test on the Security Request page.
Enable reCAPTCHA for login page	Select to display a reCAPTCHA human verification response test on the Web PhoneManager logon page.
reCAPTCHA™ API Public Key Code (See Note)	Enter the reCAPTCHA Public Key Code. If you use a reCAPTCHA Code, subscribers must enter the code to complete the security code reset transaction.
reCAPTCHA™ API Private Key Code (See Note)	Enter the reCAPTCHA Private Key Code. If you use a reCAPTCHA Code, subscribers must enter the code to complete the security code reset transaction.

NOTE Web PhoneManager uses reCAPTCHA v2, a free service from Google that is used on many websites as a security measure to prevent abuse from automated computer programs. Users are required to select the I'm not a robot check box (and in some cases, validate whether or not they are human by selecting images) to continue with the process of resetting their security codes. For more information, or to obtain free reCAPTCHA keys for your website, visit <https://www.google.com/recaptcha/intro/>.

Expose Availability Settings to Subscribers	Description
Expose Availability Settings to Subscribers	Allow subscribers to see and use Availability Settings if their accounts are enabled and allowed. All of these settings are enabled by default.
Enable Availability Processing setting	Select to enable or clear to disable the Availability Processing setting.
Announce Availability settings	Select to control the ability to toggle the Announce Availability settings from the Availability States tab of Availability Settings .
Find-me Devices settings	Select to enable or clear to disable the Find-me Devices settings. If enabled, Find Me Devices and Locate Mode can be edited in the Availability States tab of Availability Settings .
Allow Call Alert notification for mobile client devices	Select to control the ability to toggle the Call Alert notification for mobile client devices setting from the Availability States tab of Availability Settings .
Enable Call Screening	Select to enable or clear to disable call screening.

Route to Subscriber settings	Select to enable or clear to disable the Route to Subscriber settings.
Message Acceptance setting	Select to control the ability to toggle the Accept Messages setting from the Availability Settings .
Device Types	Select to enable or clear to disable the Device Types setting. If enabled, this allows for the ability to edit the Devices settings in the Phone Number tab of the Personal Settings section.
SAML SSO	Description
SAML SSO	Settings related to Security Assertion Markup Language (SAML) Single Sign On (SSO). These settings are not enabled by default.
IdP Metadata URL	Enter the URL for the Identity Provider (IdP) Metadata.
IdP Target URL	Enter the target URL for the IdP (Identity Provider).
IdP Certificate	Paste the IdP Certificate in this box.
Assertion URL	Enter the Assertion Uniform Resource Locator (URL).
Application Identifier	Enter the Application Identifier.
WebServices UserID	Enter the WebServices UserID.
WebServices Password	Enter the WebServices password.

Updating the Web PhoneManager Dashboard Tab

You can post information of general interest to your subscribers on the **Dashboard** tab of the **Home** folder of Web PhoneManager, where they are likely to see it. For example, you might want the **Dashboard** tab to display the following items:

- Announcements of upcoming changes or service to the MiCollab AM server or other network resources
- Reminders of upcoming events such as meetings, gatherings, and deadlines
- Contact information for departments or personnel within the organization

The **Dashboard** tab is configured with the **dashboard.xml** file. The **dashboard.xml** file and the **dashboard_sample.xml** file, are located in the Web PhoneManager root directory.

The **dashboard_sample.xml** file provides a layout example for the information on the **Dashboard** tab.

In addition, the **dashboard.xml** file allows you to add information to the logon page. The text appears on the logon dialog box above the mailbox field, and/or below the **Login** button, depending on how you configure the file. For example, you might want the Logon page to display the following items:

- The organization's primary access number and extension number for MiCollab AM
- The telephone number and e-mail address of the organization's help desk

NOTE To format your information in the following procedure, you can use inline HTML formatting tags such as **** (boldface), **<i>** (italic) and **<u>** (underline), as well as HTML entity references. However, remember that the file is actually an XML file and that all tags of any kind must be properly closed. For example, every **<p>** tag must have a corresponding **</p>** tag.

To post information on the Dashboard tab (optional):

- 1 Use an XML or text editor to open the **dashboard.xml** file in the Web PhoneManager root directory.

IMPORTANT As you edit the dashboard.xml file, do not disturb the CDATA labels or any of the square brackets associated with them. Put your information between the square brackets. For example, **<![CDATA[Insert your text here]]>**.

- 2 Between the **<name>** and **</name>** tags, replace the existing name with the organization's company name.

For example:

```
<name>
<![CDATA[My company name]]>
</name>
```

- 3 Between the **<logo>** and **</logo>** tags, replace the existing path with a valid path to the organization's logo.

For example:

```
<logo>images/companylogo.png</logo>
```

NOTE If your organization's logo is too large, it may distort the layout of the Web PhoneManager page. If this happens, reduce the size of your logo until the Web PhoneManager page displays correctly. It is recommended that you use either a transparent **.gif** or **.png** file for your company logo on the Web PhoneManager page.

- 4 Between the **<message>** and **</message>** tags, modify the dashboard message content as appropriate for your organization.

For example:

```
<message>
<![CDATA[Welcome to the Web PhoneManager Unified Communications Portal!]]> </message>
```


- 5 Save the file.

To post text on the Logon page (optional):

- 1 Use an XML or text editor to open the **dashboard.xml** file in the Web PhoneManager root directory.

IMPORTANT As you edit the dashboard.xml file, do not disturb the CDATA labels or any of the square brackets associated with them. Put your information between the square brackets. For example, `<![CDATA[Insert your text here]]>`.

- 2 Between the `<login_message_top>` and `</login_message_top>` tags, modify the text as appropriate for your organization. The text appears on the logon dialog box above the mailbox field.

For example:

```
<login_message_top>
<![CDATA[Dial 415 555 1234 or Ext. 6000 to reach Voicemail]]>
</login_message_top>
```

- 3 Between the `<login_message_bottom>` and `</login_message_bottom>` tags, modify the text as appropriate for your organization. The text appears on the logon dialog box below the **Login** button.

For example:

```
<login_message_bottom>
<![CDATA[Help Desk 415 555 1250 or helpdesk@company.com]]>
</login_message_bottom>
```

- 4 Save the file.

Updating the Administrator's Contact Information

If you are using the **Security Code Reset** feature, you should configure the administrator's contact information to suit your organization's requirements. The contact information displays on the **E-mail Sent** page after the subscriber successfully requests a security code reset, and MiCollab AM sends an e-mail to the subscriber.

NOTE For more information on configuring MiCollab AM and Web PhoneManager to use the Security Code Reset feature, refer to the *System Administration Guide* or the MiCollab AM online help topic, *Configuring the Security Code Reset Feature*.

The contact information is configured with the **contact_admin.xml** file. The **contact_admin_sample.xml** file provides a layout example for the information on the **E-mail Sent** page. The **contact_admin.xml** file and the **contact_admin_sample.xml** file are located in the Web PhoneManager root directory.

For example:

```
C:\inetpub\WPM
```

You can change any information within the red text box of this example by editing the **contact_admin.xml** file.

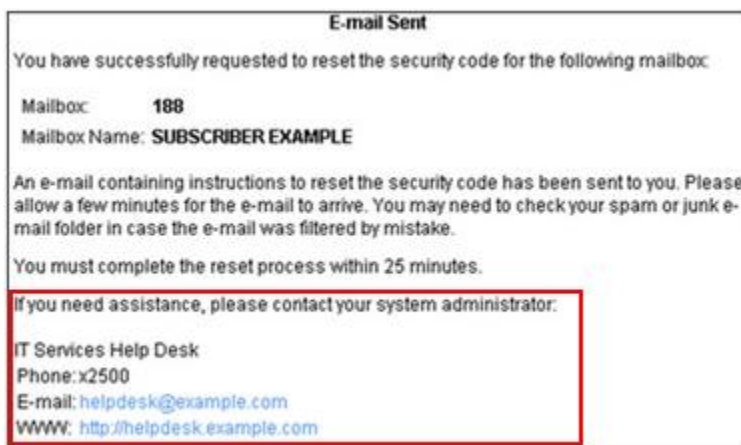


Figure 5. E-mail Sent Page

To change the contact information for your organization:

- 1 Use an XML or text editor to open the **contact_admin.xml** file in the Web PhoneManager root directory.

IMPORTANT As you edit the **contact_admin.xml** file, do not disturb the CDATA labels or any of the square brackets associated with them. Put your information between the square brackets. For example, `<![CDATA[Insert your text here]]>`.

- 2 Enter the contact telephone number between the phone number `<td>` `</td>` tags.
For example:
`<td>Phone:</td>`
`<td>415 555 1250 or Ext 1250</td>`
- 3 Enter the contact e-mail address between the e-mail address `<td>` `</td>` tags. It is not necessary to remove the href tags.
For example:
`<td>E-mail:</td>`
`<td>`
`helpdesk@example.com</td>`
- 4 Enter the help desk web address between the WWW: `<td>` `</td>` tags. It is not necessary to remove the href tags.
For example:
`<td>WWW:</td>`
`<td>`
`http://helpdesk.company.com</td>`
- 5 Save the file.

Removing or Renaming the admin.php file for Added Security

Once you have completed the Web Phone Manager configuration, you can rename or remove the **admin.php** file from your web server to guard against unauthorized changes to the Web Phone Manager configuration.

IMPORTANT The **admin.php** file can pose a security risk to your Web PhoneManager system if an unauthorized person gains access to it. For added security, you can also set the permissions for the config file in [Changing the Permissions of the Configuration Directory](#) to a read-only setting.

NOTE If you are installing Message Cache Manager to operate with Web PhoneManager, you must also configure the Message Cache Manager Server's address in the Web PhoneManager configuration. The easiest way to configure this server address is from the **admin.php** web page so you may want to wait to rename or delete the **admin.php** file until you have successfully installed and configured Message Cache Manager.

To remove or rename your admin.php file:

- 1 Navigate to the folder on your web server that contains the **admin.php** file.
- 2 Select the **admin.php** file and rename it. Alternatively, you can delete the file.

NOTE If you delete the **admin.php** file and need to access it again, you can copy the **admin.php** file from the MiCollab AM Installation Media to the appropriate folder on your web server.

Configuring Client Workstations

Provide subscribers with the following information to ensure they can use Web PhoneManager successfully:

- The web address (URL) of where they can log in to Web PhoneManager
For example:
http://domain/wpm
where **domain** is the domain name you assigned to the Web PhoneManager web server.
- The required browser settings listed in the following table:

Table 13. Browser Settings

Browser	Settings
Internet Explorer	Allow cookies Enable Active Scripting*
Firefox, Opera, and Safari	Enable all cookies Enable JavaScript*
* This setting is not required but is recommended if the organization allows the use of JavaScript. Screen presentation, page refresh, and logout confirmation work more smoothly if JavaScript is enabled. In addition, the AJAX interface does not work correctly if JavaScript is disabled. It is recommended that you enable the AJAX interface in order to benefit from the full functionality of the web client.	

- Optionally, if you make the Web PhoneManager URL accessible from outside the organization, your subscribers can use Web PhoneManager to keep up to date on their messages from anywhere: in the office, at home, and on the road.

Installing Message Cache Manager

Message Cache Manager is a Windows Service that acts as a liaison between Web PhoneManager and the MiCollab AM System Server. It reduces traffic between Web PhoneManager and the MiCollab AM SOAP server, thus reducing processing overhead on the System Server.

The private key and cert pair for SSL encrypted communication is generated automatically using OpenSSL during the MiCollab AM installation. These files are saved in the **CX/Bin** folder in the **server.pem** file. These keys are 2048-bit keys and are not encrypted. If the keys already exist, they are not overwritten.

You can reconfigure Ports on the SOAP server by editing the file, **AT_SOAPServer.xml**.

Message Cache Manager can run on the same platform as Web PhoneManager, on a stand-alone server, or on any shared server on the network. The server on which you install Message Cache Manager must be able to communicate through a network connection with all Web PhoneManager servers and all System Servers with which it is integrated.

The server on which you install Message Cache Manager depends on:

- The amount of subscriber traffic the Web Phone Manager server experiences
- How many Web PhoneManager servers connect to the System Server through Message Cache Manager
- How many System Servers connect to the Message Cache Manager

Choose a server whose current processing overhead is lower than other servers within the network. For deployments in large, high traffic enterprises, it may be necessary to install Message Cache Manager on a stand-alone server.

For more information, refer to [Message Cache Manager Server Requirements](#).

To install Message Cache Manager:

- 1 Log on to the server platform using a Windows Administrator account.
- 2 Shut down all other applications.
- 3 Insert the MiCollab AM Installation Media into the appropriate drive of your server.
- 4 Do one of the following:

Table 14. Autorun Options

If autorun is...	Then...
Enabled	<ol style="list-style-type: none">① In the Server Components area, select Message Cache Manager.② The Install Shield Wizard for Message Cache Manager appears.
Not Enabled	<ol style="list-style-type: none">① Go to Start > My Computer, and then double-click the drive where the MiCollab AM Installation Media is inserted.

- ② Browse to the **Server Components** area, select **Message Cache Manager**, and then double-click **Setup**.
 - ③ The **Install Shield Wizard for Message Cache Manager** appears.
-

- 5 Click **Next**. The **License Agreement** dialog box appears.
- 6 Click **Yes** to accept the license agreement. The **Choose Destination** dialog box appears.
- 7 Click **Next** if the default destination folder is acceptable, or click **Browse** to select a new destination location, and then click **Next**. The **Review settings** dialog box appears.
- 8 Click **Next**. The installation starts. When finished, the **Message Cache Manager Initialization** dialog box appears.

NOTE Configure the initial System Server in **Steps 9** through **11**. You can add System Servers later using the Message Cache Manager Configuration. For more information, refer to the next section, [Configuring Message Cache Manager](#).

- 9 In the **Server address** field, enter the TCP/IP address or the FQDN of the System Server
- 10 In the **Administrator** field, enter the MiCollab AM administrator's log on ID for the System Server.
- 11 In the **Password** field, enter the MiCollab AM administrator's password.

NOTE Alternatively, if you want Message Cache Manager to use a Windows domain administrator account to log on to the System Server, select the **Windows Integrated Logon** box.

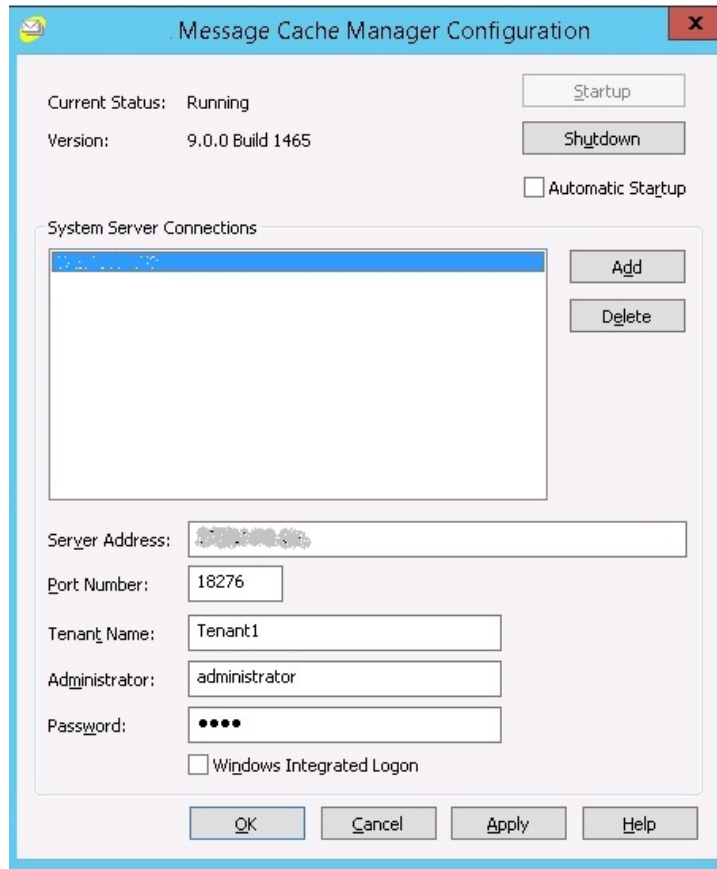
- 12 Click **Next**. The **Install Shield Wizard** dialog box appears.
- 13 Click **Finish**. The installation is complete.

Configuring Message Cache Manager

The Message Cache Manager Configuration utility allows you to start and shut down the Service, edit the configuration, or add additional System Servers to Message Cache Manager.

To run Message Cache Manager Configuration:

- 1 Go to **Start > All Programs > MiCollab AM Desktop**, and then select **Message Cache Manager**. The Message Cache Manager Configuration utility appears.



The following table provides a description for each field and button of the **Message Cache Manager Configuration** utility.

Table 15. Message Cache Manager Configuration Utility Field Descriptions

Field	Description
Current Status	Displays the current status of the Message Cache Manager.
Version	Displays the current Message Cache Manager software version and build.
Startup button	Click Startup to start the Message Cache Manager Service.
Shutdown button	Click Shutdown to stop the Message Cache Manager Service.
Automatic Startup	Select to start the Message Cache Manager Service automatically during system start-up. It is recommended that you enable the Service to start automatically.
System Server Connections	Lists the System Servers currently configured. To view or edit the current settings, highlight the System Server in the list. The settings for the server display.

Add	Click Add to add a System Server to the configuration.
Delete	To remove a System Server from the list, highlight the System Server, and then click Delete .
NOTE Only additional System Servers can be deleted; the initial System Server configuration can only be edited.	
Server Address	The TCP/IP address or the FQDN of the System Server
Port number	The TCP port number Message Cache Manager uses to communicate with the System Server.
Tenant Name	<p>The name of the Tenant.</p> <p>If the same MiCollab AM server hosts multiple tenants, you can create multiple entries for the same server with different Tenant Names. For a multi-tenanted system, the Tenant Name field is mandatory and a Tenant Name must be entered. The Tenant Name is not mandatory for a single tenanted system.</p>
Administrator	The MiCollab AM administrator's user ID
Password	The MiCollab AM administrator's password
Windows Integrated Logon	Select to use the Windows domain log on ID to log onto MiCollab AM

Configuring Web PhoneManager for Message Cache Manager

Once Message Cache Manager is running, you must configure Web PhoneManager to communicate with it. There are two ways you can modify the Web PhoneManager configuration.

- Follow the steps in the section [Configuring Web PhoneManager](#) to log in to Web PhoneManager and open the **admin.php** file. In the **Message Cache Manager Address** field of **admin.php**, enter the Message Cache Manager Server's FQDN or IP address.
- Follow the steps in [Appendix A – Configuring Web PhoneManager with an XML or Text Editor](#) to edit the configuration with an XML or Text Editor. Enter the Message Cache Manager Server's FQDN or the IP Address between the **message_cache_manager** tags.

Starting Message Cache Manager

Once you have configured Message Cache Manager to communicate with the System Server and you have configured Web PhoneManager to communicate with the Message Cache Manager server, you can start Message Cache Manager.

To start Message Cache Manager:

- 1 On the Message Cache Manager Configuration utility, click **Start**.
- 2 If you want Message Cache Manager to start automatically during system start-up, select **Automatic Startup**.
- 3 Click **OK** to save and close the Message Cache Manager Configuration utility.

Appendix A – Configuring Web PhoneManager with an XML or Text Editor

You can modify the Web PhoneManager configuration by editing the `config.xml` file with an XML or text editing program. The `config.xml` file contains the same list of parameters that displays on the `admin.php` web page. The `config_defaults.xml` file is a default file of the `config.xml` file and provides an example, or a return to default, of the `config.xml` file. The following procedure describes how to make these modifications using an XML or text editor.

To configure Web PhoneManager with a text editor:

- 1 Use an XML or text editor to open the `config.xml` file in the `config` sub-directory of the Web PhoneManager root directory.

IMPORTANT As you edit the `config.xml` file, do not disturb the tag structure. Edit only the configuration information between the tags.

For example:

```
<call_xpress name="San Francisco">sample.domain.com</call_xpress>.
```

```
<?xml version="1.0"?>
<!DOCTYPE WPMConfig SYSTEM "config.dtd">
-<WPMConfig>
  -<servers>
    <message_cache_manager/>
    <call_xpress tenant-name="#" name="CX Server">CX_SERVER</call_xpress>
    <soap_protocol>http</soap_protocol>
    <cxxml_namespace>http://www.mitel.com/CXIf</cxxml_namespace>
  </servers>
  -<application>
    <root>main.php</root>
    <default_module>home</default_module>
    <default_language>en</default_language>
    <allow_ajax>1</allow_ajax>
    <allow_stream_audio>1</allow_stream_audio>
    <allow_download_audio>1</allow_download_audio>
    <allow_full_directory>1</allow_full_directory>
    <allow_save_login>1</allow_save_login>
    <save_login_days>2</save_login_days>
    <exit_purge_messages>0</exit_purge_messages>
    <refresh_list>5</refresh_list>
```

```

<default_playback>stream</default_playback>
<allow_personal_operator>1</allow_personal_operator>
<allow_trusted_setting>0</allow_trusted_setting>
<playback_speed_setting_allowed>2</playback_speed_setting_allowed>
<secure_cookie_only>0</secure_cookie_only>
<allow_pw_reset>1</allow_pw_reset>
<require_all_fields_for_pw_reset>0</require_all_fields_for_pw_reset>
<show_fields_for_pw_reset>1</show_fields_for_pw_reset>
<enable_ap_for_pw_reset_page>0</enable_ap_for_pw_reset_page>
<enable_ap_for_login_page>0</enable_ap_for_login_page>
<recaptcha_public_key/>
<recaptcha_private_key/>
<expose_enable_avail_processing>1</expose_enable_avail_processing>
<expose_announce_avail>1</expose_announce_avail>
<expose_message_acceptance>1</expose_message_acceptance>
<expose_find_me_devices>1</expose_find_me_devices>
<expose_route_to_subscriber>1</expose_route_to_subscriber>
<expose_device_types>1</expose_device_types>
<allow_call_alert_mobile>1</allow_call_alert_mobile>
<enable_call_screening_non_mobile>1</enable_call_screening_non_mobile>
<saml_idp_target_url/>
<saml_idp_metadata_url/>
<saml_certificate/>
<saml_assertion_url/>
<saml_app_identifier/>
<webservices_userid/>
</application>
-<paths>
  <localizations>lang</localizations>
  <modules>modules</modules>
  <tools>tools</tools>
  <help>help</help>
  <resources>resources</resources>
</paths>
</WPMConfig>

```

- 2 In the <servers> section of the file, modify the values stored in each tag and the attributes assigned to each one, as shown in the following table.

Table 16. Web PhoneManager config.xml - Servers

Tag	Attribute Name and Tag Value
<message_cache_manager>	Enter the FQDN or the IP address of the Message Cache Server. For example: <message_cache_manager>192.168.1.125</message_cache_manager>

<call_xpress>	<p>Enter the System Server name that you want Web PhoneManager to display, and then enter the System Server address.</p> <p>The Server name and the FQDN or IP Address of the System Server platform.</p> <div> <p>NOTE If you want your subscribers to select from multiple System Servers, create multiple <call_xpress> tags in this file.</p> <p>For example: The following tags would allow users to select one of two System Servers to log on to their mailboxes: <call_xpress name="Seattle">192.168.1.125</call_xpress> <call_xpress name="San Francisco">sf.domain.com</call_xpress></p> </div>
<soap_protocol>	<p>Enter the transmission protocol. The two options are http (default) and https. Https enables SSL encryption to the SOAP server.</p> <div> <p>For example: <soap_protocol>https</soap_protocol></p> </div>
cxxml_name_space>	<p>The URL of the XSL namespace definition for Web PhoneManager (currently www.mitel.com)</p> <div> <p>IMPORTANT Do not modify this value.</p> </div>

- 3** In the <application> section of the file, modify the values of any tags for your organization's needs, as shown in the following table.

Table 17. Web PhoneManager Config.xml Application

Tag	Attribute Name and Tag Value
<root>	<p>The root is the filename of the first web page that the browser loads for Web PhoneManager subscribers.</p> <div> <p>For example: <root>main.php</root></p> <p>IMPORTANT Most organizations should not change this value.</p> </div>
<default_module>	<p>The subdirectory name (within the Modules directory) of the first page you want to display to subscribers when Web PhoneManager starts, as follows:</p>

	<p> home (Home page Inbox tab, the default) documentation (User Resources page) message (Message Settings page) notifications (Notification Settings page) personal (Personal Settings page) settings (Web PhoneManager Settings page) speech (Speech Settings page) </p> <p>For example:</p> <pre><default_module>home</default_module></pre>
<default_language>	<p>Enter the two-letter abbreviation for the default language in which Web PhoneManager displays.</p> <p>NOTE You must specify a language that Web PhoneManager currently supports. For a list of two-letter language codes, refer to Codes for the Representation of Names of Languages.</p> <p>For example:</p> <pre><default_language>en</default_language></pre>
<allow_ajax>	<p>Enable or disable the AJAX (asynchronous JavaScript and XML) interface.</p> <ul style="list-style-type: none"> • 1 or TRUE: Activates the feature (default) • 0 or any other value: Deactivates the feature <p>NOTE Mitel recommends that you keep the JavaScript/AJAX interface enabled. Disabling the JavaScript/AJAX interface disables streaming playback as well as other features of Web PhoneManager.</p> <p>For example:</p> <pre><allow_ajax>1</allow_ajax></pre>
<allow_stream_audio>	<p>Enable or disable the ability of streaming message playback to subscribers.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>NOTE Streaming message playback does not require installation of Adobe Flash.</p> <p>For example:</p> <pre>< allow_stream_audio>1</allow_ stream_audio></pre>
<allow_download_audio>	<p>Enable or disable the ability of message downloading and local playback to the subscriber's workstation. This</p>

	<p>feature allows subscribers without access to streaming playback or a telephone to listen to their messages, at the cost of reduced security.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example:</p> <pre><allow_download_audio>1</allow_download_audio></pre>
<code><allow_full_directory></code>	<p>Enable or disable the ability of blank directory searching for subscribers. This feature allows a subscriber who is sending or forwarding a message to click the Search button without first specifying a name to find.</p> <p>If the feature is active, this search displays all mailboxes available on MiCollab AM in the left column of the message-recording panel. If the feature is inactive, the Search button has no effect until the subscriber types a name in the adjacent box.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example:</p> <pre><allow_full_directory>1</allow_full_directory></pre>
<code><allow_save_login></code>	<p>Enable or disable the ability of login persistence to subscribers. This feature allows Web PhoneManager to preserve the context in which subscribers are working when they exit their browsers. The next time the subscribers log in, Web PhoneManager picks up where it left off with them.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p>NOTE When this feature is active, a subscriber must select the Remember me on this computer box on the login page to use it.</p> </div> <p>For example:</p> <pre><allow_save_login>1</allow_save_login></pre>
<code><save_login_days></code>	<p>Enter the number of days that a subscriber's login information persists. The default is two days.</p> <p>For example:</p> <pre><save_login_days>2</save_login_days></pre>
<code><exit_purge_messages></code>	<p>Enable or disable the ability of the system to purge deleted messages when a user exits Web PhoneManager.</p>

	<ul style="list-style-type: none"> • 1 or TRUE: Activates the feature • 0 (default) or any other value: Deactivates the feature <p>For example: <exit_purge_messages>0</exit_purge_messages></p>
<refresh_list>	<p>Enter the number of minutes that pass before Web PhoneManager refreshes a user's message list. The default is five minutes.</p> <p>For example: <refresh_list>5</refresh_list></p>
<default_playback>	<p>Enter the default message-playback type for Web PhoneManager. The playback options include: stream (default), telephone, or download.</p> <div> <p>NOTE The use of the word flash will set streaming message playback as the default, but this does not require installation of Adobe Flash.</p> </div> <p>For example: <default_playback>stream</default_playback></p>
<allow_personal_operator>	<p>Enable or disable the users' ability in Web PhoneManager to edit the Personal Operator field.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example: <allow_personal_operator>1</allow_personal_operator></p>
<allow_trusted_setting>	<p>Enable or disable the users' ability in Web PhoneManager to set a device as trusted or auto logon.</p> <ul style="list-style-type: none"> • 1 or TRUE: Activates this feature • 0 (default) or any other value: Deactivates the feature <p>For example: <allow_trusted_setting>0</allow_trusted_setting></p> <div> <p>IMPORTANT The MiCollab AM administrator must configure MiCollab AM to allow trusted logons before subscribers can configure a device as trusted. For more information, refer to the MiCollab AM help topic <i>Allowing Trusted Logons</i>.</p> </div>

NOTE When a device is set as trusted, a call made directly from the device number to MiCollab AM automatically logs the subscriber on to their MiCollab AM mailbox, thereby skipping the entry of the security code. This is also known as auto logon.

<playback_speed_setting_allowed>	<p>Enable or disable subscriber's ability to use the playback speed mechanism during a Message Session or not (none). The default is 2, Message, Session enabled.</p> <p>For example: <playback_speed_setting_allowed>2</playback_speed_setting_allowed></p>
<secure_cookie_only>	<p>Enable or disable the cookie for SSL (HTTPS). When enabled the subscriber's browser can only send a cookie to Web Phone Manager using SSL (Secure Socket Layer).</p> <ul style="list-style-type: none"> • 1 (default) or TRUE: Activates the feature • 0 or any other value: Deactivates the feature <p>For example: <secure_cookie_only>1</secure_cookie_only></p> <p>NOTE If the Web PhoneManager site is not using SSL or HTTPS, do not enable the Secure Cookie Flag. Subscribers are unable to access Web PhoneManager if this flag is enabled and you are not using SSL.</p>
<allow_pw_reset>	<p>Enable or disable the Security Code Reset feature the Forgot Security Code? link) on the logon page and on the Security Code tab of the Personal Settings page.</p> <ul style="list-style-type: none"> • 1 (default) or TRUE: Activates the feature • 0 or any other value: Deactivates the feature <p>For example: <allow_pw_reset>1</allow_pw_reset></p>
<require_all_fields_for_pw_reset>	<p>Enable or disable the ability to require all fields for the Security Code Reset feature on the Security Code Reset Request page.</p> <ul style="list-style-type: none"> • 1 or TRUE: Activates the feature • 0 (default) or any other value: Deactivates the feature <p>For example:</p>

	<pre><require_all_fields_for_pw_reset>0</require_all_fields_for_pw_reset></pre>
<code><show_fields_for_pw_reset></code>	<p>Enable or disable the ability to display the Mailbox ID and Mailbox Name after a successful security code reset link has been generated using the Security Code Reset feature.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example: <pre><show_fields_for_pw_reset>1</show_fields_for_pw_reset></pre></p>
<code><enable_ap_for_pw_reset_page></code>	<p>Enable or disable Google reCAPTCHA for the Security Code Reset page, if configured.</p> <ul style="list-style-type: none"> • 1 or TRUE: Activates the feature • 0 (default) or any other value: Deactivates the feature <p>For example: <pre><enable_ap_for_pw_reset_page>0</enable_ap_for_pw_reset_page></pre></p>
<code><enable_ap_for_login_page></code>	<p>Enable or disable Google reCAPTCHA for the Web PhoneManager Login page, if configured.</p> <div style="background-color: #e6f2ff; padding: 10px; margin: 10px 0;"> <p>NOTE This does not apply to Single Sign-on (SSO) logins, which are handled by the Identity Provider (IdP).</p> </div> <ul style="list-style-type: none"> • 1 or TRUE: Activates the feature • 0 (default) or any other value: Deactivates the feature <p>For example: <pre><enable_ap_for_login_page>0</enable_ap_for_login_page></pre></p>
<code><recaptcha_public_key></code>	<p>If you are using the reCAPTCHA program with the Security Code Reset feature, enter the public key code here.</p> <p>For example: <pre><recaptcha_public_key>6LHW9YSABCDEJKLxyx1DkK3kYggcZjNHjJuLK20</recaptcha_public_key></pre></p>

<recaptcha_private_key>	<p>If you are using the reCAPTCHA program with the Security Code Reset feature, enter the private key code here.</p> <p>For example: <recaptcha_private_key>6LHW9YSABCDEJKLxyx1DkK3kYggcZjNHijulK20</recaptcha_private_key></p>
<expose_enable_avail_processing>	<p>Enable or disable the ability to expose the Enable Availability Processing setting option.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example: <expose_enable_avail_processing>1</expose_enable_avail_processing></p>
<expose_announce_avail>	<p>Enable or disable the ability to expose the Announce Availability settings option.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example: <expose_announce_avail>1</expose_announce_avail></p>
<expose_message_acceptance>	<p>Enable or disable the ability to expose the Message Acceptance setting option.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example: <expose_message_acceptance>1</expose_message_acceptance></p>
<expose_find_me_devices>	<p>Enable or disable the ability to expose the Find-me Devices settings option.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example: <expose_find_me_devices>1</expose_find_me_devices></p>
<expose_route_to_subscriber>	<p>Enable or disable the ability to expose the Route to Subscriber settings option.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example:</p>

	<pre><expose_route_to_subscriber>1</expose_route_to_subscriber></pre>
<pre><expose_device_types></pre>	<p>Enable or disable the ability to expose the Device Types option.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example:</p> <pre><expose_device_types>1</expose_device_types></pre>
<pre><allow_call_alert_mobile></pre>	<p>Enable or disable the ability to expose the Allow Call Alert notification for mobile client devices option.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example:</p> <pre><allow_call_alert_mobile>1</allow_call_alert_mobile></pre>
<pre><enable_call_screening_non_mobile></pre>	<p>Enable or disable the ability to expose the Enable Call Screening option.</p> <ul style="list-style-type: none"> • 1 or TRUE (default): Activates the feature • 0 or any other value: Deactivates the feature <p>For example:</p> <pre><enable_call_screening_non_mobile>1</enable_call_screening_non_mobile></pre>
<pre><saml_idp_target_url/></pre>	<p>If you are using Single Sign-on (SSO), enter the URL of the Identity Provider (IdP) Single Sign-on (SSO) service. Refer to Appendix D – How to Configure Single Sign-On for more information.</p> <p>For example:</p> <pre><saml_idp_target_url/>http://ADFS_SERVER_NAME/adfs.ls</saml_idp_target_url ></pre>
<pre><saml_idp_metadata_url /></pre>	<p>If you are using the SAML SSO feature, enter the IdP Metadata URL here.</p> <p>For example:</p> <pre><saml_idp_metadata_url/>www.sampleurl.com</saml_idp_metadata_url ></pre>
<pre><saml_idp_certificate_url /></pre>	<p>If you are using Single Sign-on (SSO), enter the certificate the IdP uses to sign the SAML assertion here.</p> <p>For example:</p> <pre><saml_idp_certificate_url/> -----BEGIN CERTIFICATE-----</saml_idp_certificate_url ></pre>

<saml_idp_assertion_url />	<p>If you are using Single Sign-on (SSO), enter URL to the SAMLLogonComplete.php page. This should exactly match (is case-sensitive too) the URL to this page that was configured in ADFS for this Relying Party.</p> <p>For example: <saml_idp_assertion_url/>www.sampleassertionurl.com </saml_idp_assertion_url ></p>
<saml_app_identifier/>	<p>If you are using Single Sign-on (SSO), enter the identifier of the application. This should exactly match (is case-sensitive too) the identifier of the Relying Party that was configured in ADFS.</p> <p>For example: <saml_idp_metadata_url/>sampleapplicationidentifier </ saml_idp_metadata_url ></p>
<webservices_userid/>	<p>If you are using Single Sign-on (SSO), enter User ID of the MiCollab AM administrator account that will be used to log on to the SOAP server for creating a subscriber session.</p> <p>For example: <webservices_userid/>123456</webservices_userid></p>

4 Save the file.

Appendix B – Configuring the User Resources Page with an XML or Text Editor

The User Resources page in Web PhoneManager provides access to content that you would like end-users to access. For example, you might want to post a Quick Reference Card so that users can better understand the telephone user interface or a document on how to communicate with various departments and personnel within the organization.

You can modify the User Resources page by editing the resources.xml file with an XML or text editing program. The resources_sample.xml file is a default file of the resources.xml file and provides an example, or a return to default, of the resources.xml file. The following procedure describes how to make these modifications using an XML or text editor.

IMPORTANT If you add or change resources you must also make sure the target resource is in the folder you specify.

To configure the User Resources page with an XML or text editor...

- 1 Use an XML or text editor to open the resources.xml file in the resources sub-directory of the Web PhoneManager root directory.

IMPORTANT As you edit the resources.xml file, do not disturb the tag structure. Edit only the configuration information between the tags.

For example:

```
<target>WebPhoneManager/player.html</target>
```

- 2 In the <resources> section of the file, modify the values stored in each tag and the attributes assigned to each one, as shown in the following table.

Table 18. Resources.xml

Tag	Attribute Name and Tag Value
<name>	The resource name that you want the resource page to display to users. For example: <name>End-User Training</name>
<image>	The file name of an image you have stored in the resources directory. For example: <image>pdficon_small.gif</image>

<folder>	<p>The folder is the name of any subdirectory in which you are storing files in the resources folder.</p> <p>For example:</p> <p><folder>our</folder></p>
<target>	<p>The target is the filename of the resource that end-users want to display.</p> <p>For example:</p> <p><target>WebPhoneManager_user.pdf</target></p>

- 3 Save the file.

Appendix C – How to Upgrade Web PhoneManager

Upgrading Web PhoneManager entails copying the files from the installation media and overwriting the files on the web server. However, it is important to back up your original files, especially the original `config.xml` file. This will ensure that you can revert back to the original configuration, if required.

WARNING Any customizations to WPM that you have made, such as logo replacements or additional pages, will be lost as part of this upgrade. Any customizations must be manually applied after the upgrade.

To upgrade your WPM system:

- 1 Browse to your WPM files on your existing system.
- 2 Make a backup copy of the entire web directory structure.
- 3 Locate the file **config.xml** and ensure that it is contained in the backup. If using a compressed archive for backup, retain a copy of this file outside of the archive.

NOTE In MiCollab AM versions prior to 5.0, the **config.xml** file is located in the root directory. In more recent versions, it is in the config directory.

- 4 Copy the directory structure of the MiCollab AM Web PhoneManager directories to the existing web folders, overwriting any existing files.
- 5 Copy the `config.xml` file retained above to the config folder and overwrite the existing file.
- 6 Configure Web PhoneManager. Settings configured in the previous version of WPM will be retained via **config.xml**. However, you will need to configure any features not available in the previous version.

Appendix D – How to Configure Single Sign-On

Single Sign-on (SSO) support in Web PhoneManager uses the Security Assertion Markup Language (SAML) protocol. The only Identity Provider (IdP) supported at this time is Microsoft Active Directory Federation Services (ADFS) version 2.0 or above. Refer to the following instructions on how to configure ADFS, MiCollab AM, and WPM for SSO.

Setting up ADFS 2.0 to Work with WPM SSO

To set up ADFS 2.0 to work with WPM SSO:

- 1 In ADFS Admin, go to **Trust Relationships > Relying Party Trusts**. Right-click and select **Add Relying Party Trust...** Start the wizard.
- 2 When the wizard asks for the option to be used to obtain data, select **Enter data about the relying party manually** and then click **Next**.
- 3 Enter a display name and click **Next**.
- 4 Choose **AD FS 2.0 profile** and click **Next**.
- 5 Skip entering a token encryption certificate and click **Next**.
- 6 Choose **Enable support for the SAML 2.0 WebSSO protocol** and for the SSO service URL enter the URL for the SAMLLogonComplete.php page.
Example SSO service URL:
<https://www.company.com/wpm/SAMLLogonComplete.php>
- 7 Click **Next**.
- 8 For the identifier for this Relying Party, enter a unique name.
For example:
You could concatenate the machine name of the WPM server and the application name and create an identifier such as **WEBSERVER1-WPM**. You could also let this be a URL such as a URL of the WPM machine.
- 9 Click **Add** and then click **Next**.
- 10 Select **Permit all users to access this relying party**.
- 11 Click **Next** in the **Ready to Add Trust** screen.
- 12 The Relying Party Trust has been created. If you selected the **Open Edit Claim Rules** option, you will automatically go into the next step. Otherwise, right-click on the **Relying Party Trust** you just created and choose **Edit Claim Rules...**

- 13 On the **Issuance Transform Rules** tab, select **Add Rule...**
- 14 Select **Send LDAP Attribute as Claims** as the claim rule template to use and then click **Next**.
- 15 Give the Claim a name such as *Get LDAP Attributes*. Attribute Store should be set to **Active Directory**, **LDAP Attribute** should be **E-Mail-Addresses**, and the **Outgoing Claim Type** should be **E-mail Address**.
- 16 Click **Finish**.
- 17 Once again, select **Add Rule...** to add another Rule.
- 18 Select **Transform an Incoming Claim** as the claim rule template to use for this Rule and click **Next**.
- 19 Give it a name such as *Email to Name ID*.

The incoming claim type should be **E-mail Address** (it must match the **Outgoing Claim Type** configured in rule #1).

Outgoing claim type is **Name ID** (which maps to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress) and **Outgoing name ID** format is **Email**.
- 20 Select **Pass through all claim values** and click **Finish**.
- 21 Click **OK** to return to the main ADFS screen.
- 22 ADFS configuration is now complete.

Setting up MiCollab AM to Support SSO

To set up MiCollab AM to support SSO:

- 1 Open **MiCollab AM Admin** and create a new MiCollab AM administrator account that will be used by WPM to perform logons to the appropriate subscriber mailbox during an SSO logon. Give the account a distinctive name such as *WPM SSO* and add a **Comment** such as *Used by WPM - DO NOT DELETE* to help avoid accidental deletion in the future.
- 2 Open **MiCollab AM Configuration**, and then select the **Tenant** tab.
- 3 Select the tenant from the table, and then click the **Edit** button. The **Tenant Summary** dialog box appears.
- 4 In the **Web Services Impersonation** section, set the **User ID** to the MiCollab AM administrator account created in **Step 1** above.

NOTE The Web Services Impersonation covers only the mailboxes of the tenant for which it was set.

- 5 For each subscriber that will be using SSO you must configure their e-mail address in the **E-mail** field on the **Main** tab of their subscriber mailbox. The e-mail address must be the same e-mail address that the IdP resolves the user to.

Setting up WPM SSO to Work with ADFS 2.0

To configure WPM for SSO, you must open the admin.php page and log on with an administrator account. The admin.php page will add the new settings to the WPM configuration file automatically.

NOTE If configured, you can now go to an IdP Metadata URL by entering the URL in the field. Click **Fetch IdP Information** to automatically fetch the correct IdP Target URL and IdP Certificate settings. These settings can also be configured manually.

From the WPM admin.php page, set the following settings:

Table 19. Admin.php and Config.xml Settings

Admin.php Setting	Description	Config.xml Setting
IdP Target URL	The URL of the Identity Provider (IdP) Single Sign-on (SSO) service. For ADFS, the URL will typically be something like <code>http://ADFS_SERVER_NAME/adfs/ls</code> .	saml_idp_target_url
IdP Certificate	<p>The certificate the IdP uses to sign the SAML assertion. To obtain the certificate from ADFS, open the URL to the metadata of the ADFS service. The relative path to the metadata will be:</p> <p><code>/FederationMetadata/2007-06/FederationMetadata.xml</code></p> <p>Within the xml, find the tag named <i>IDPSSODescriptor</i>. Within this section, find a <i>KeyDescriptor</i> tag with an attribute, <i>use = signing</i>. This sub-section will have the <i>X509Certificate</i> that will be used to validate the signatures coming from this Identity Provider. Copy the certificate information from this tag into WPM.</p> <p>This info needs to be entered into this field in the PEM format. Please make sure of the following:</p> <p>To obtain the certificate from ADFS:</p> <ol style="list-style-type: none">1 <code>-----BEGIN CERTIFICATE-----</code> marker precedes the data.2 <code>-----END CERTIFICATE-----</code> marker follows the data3 The data in between the two markers needs to be separated out into lines with each line containing 64 characters (the last line may be less than 64 characters). <p>For example:</p> <p><code>-----BEGIN CERTIFICATE-----</code></p>	saml_certificate

MIIDAJCCAmSCEEakM712H2pJ5qjDp/WFQPUwD
 QYJKoZlHvcNAQEFBQAwwcExCzAJ
 BgNVBAYTAIVTMrcwFQYDVQQKEw5WZXJpU2ln
 biwgSW5jLjE8MDo
 GA1UECXMzQ2xh
 c3MgMyBQdWJsaWMgUHJpbWFyeSBDZXJ0aWZ
 pY2F0aW9uIEF1dGhvcml0eSAtIEcy
 MTowOAYDVQQLEzEoYykgMTk5
 OCBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3Jp
 emVklHVzZSBvbmx
 5MR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCB
 OZXR3b3JrMB4XDTk4M
 DUxODAwMDAwMFOXDTE4MDUxODIzNTk1OV0
 wgcExCzAJBgNVBAYTAIVTMrcw
 FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA
 1UECXMzQ2xhc3
 MgMyBQdWJsaWMg
 UHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml
 l0e
 SAtIEcyMTowOAYDVQQLEzEo
 YykgMTk5OCBWZXJpU2lnbiwgSW5jLiAtIEZ
 vciBhdXRob3JpemVklHVzZSBvbmx5
 MR8wHQYDVQQLExZWZXJpU2lnbiBUc
 nVzdCB0ZXR3b3JrMIGfMA0GCSqGSIb3DQEB
 AQUAA4GNADCBiQKBgQ
 DMXtERXVxp0KvTuWpMmR9ZmDCOFoUgRm1H
 P9SFIIThbbP4
 pO0M8RcPO/mn+SXXwc+EY/J8Y8+iR/LGWzOOZ
 EAEaMGAuWQcRXfH2G71ISk8UOg0
 13gfgLptQ5GVj0VXXn7F+8qkBOvqlzdUMG+7AU
 cyM83cV5tk
 aWH4mx0ciU9cZwID
 AQABMA0GCSqGSIb3DQEBBQUAA4GBABB79Ik

Assertion URL	The URL to the SAMLLogonComplete.php page. This should exactly match (is case-sensitive too) the URL to this page that was configured in ADFS for this Relying Party.	saml_assertion_url
Application Identifier	The identifier of the application. This should exactly match (is case-sensitive too) the identifier of the Relying Party that was configured in ADFS.	saml_app_identifier
WebServices UserID	The User ID of the MiCollab AM administrator account that will be used to log on to the SOAP server for creating a subscriber session.	webservices_userid

WebServices Password	<p>The password of the MiCollab AM administrator account that will be used to log on to the SOAP server for creating a subscriber session.</p> <p>The password is stored encoded. As such, you must use the admin.php page to set the password.</p>	webservices_password
-------------------------	---	----------------------
