

MiCollab Advanced Messaging Web Client Administration Guide

For version 6.1 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 2016, 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 the MiCollab AM Web Client?	8
MiCollab AM Web Client Features	8
How It Works	9
Secure Sockets Layer (SSL) and Certificates	9
Message Cache Manager	10
Before Installing the MiCollab AM Web Client	12
Web Server Installation Requirements	12
Site Requirements	12
Microsoft Web Server Requirements	12
Microsoft Windows-Based Apache Web Server Requirements	12
Linux-Based Apache Web Server Requirements	13
Message Cache Manager Server Requirements	13
Workstation Installation Requirements	13
Installing the MiCollab AM Web Client	14
Installing the Web Server Software and Other Required Software	14
Configuring IIS	14
Configuring Apache Server	15
Installing the PHP Interpreter	15
Creating Working Folders in the PHP Directory	16
Editing the PHP.ini File (Linux)	16
Testing the PHP Interpreter	17
Changing the Permissions of the Configuration Directory	18
Configuring the Firewall	19

Installing the MiCollab AM Web Client	19
Configuring the MiCollab AM Web Client	21
Configuring Server Settings	21
Changing the Logo Image	22
Linking a URL to Logo	22
Changing the Application Name	23
Configuring Time Format	23
Removing or Renaming the admin.php File for Added Security	24
Configuring Subscriber's Web Browsers	25
Installing Message Cache Manager	26
Server Requirements for Message Cache Manager	26
Configuring Message Cache Manager	27
Configuring the MiCollab AM Web Client for Message Cache Manager	29
Starting Message Cache Manager	29
Appendix A – Configuring the MiCollab AM Web Client with an XML/Text Editor	30
Appendix B – Upgrading the MiCollab AM Web Client	35

Preface

This administration guide describes how to implement the MiCollab Advanced Messaging (MiCollab AM) web client in an organization and assumes that MiCollab AM version 6.1 is running successfully. It contains the following:

- An overview of the MiCollab AM web client
- Installation requirements for your web server and client workstations
- Instructions for preparing your web server to support the MiCollab AM web client
- Instructions for installing and configuring the MiCollab AM web client
- Instructions for installing and configuring SSL Certificates
- Instructions for installing and configuring Message Cache Manager

To implement the MiCollab AM web client in an organization successfully, 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 prior to the implementation of the MiCollab AM web client.

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 documentation set for this MiCollab AM includes the following documents and resources:

- **Developer Resources.** Contains programming guides and API references for developers for integrating the server clients and web applications with MiCollab AM.
- **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.

- **Quick Reference Card (QRC).** Contains shortcuts and quick instructions telling subscribers how to access and use the messaging system.
- **Server Documentation.** Available as a PDF only. Contains administrative guides for administrators about installing, configuring, and administering the messaging system, and user guides for subscribers about accessing the messaging system and checking and sending messages.
- **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: connect.mitel.com/connect

Help

The primary source of information about MiCollab AM is the online help available within any of its administrative utilities. You can access **Help** as follows:

- Click the **Help** button in the dialog box or window in which you are working
- Press the **F1** key at any time.

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.** *Italics* fonts can also signify the titles of other documents.

Example: Refer to *System Installation Guide*.

- **UI Element Names.** Names of UI elements such as dialog windows, screens, menu items, tabs, buttons, icons, etc. are shown in bold.

Example: On the **Startup** screen, click the **Start** icon.

- **User Input.** Information required to be typed or spoken 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 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 the MiCollab AM Web Client?

The MiCollab AM web client is a web-based application that allows subscribers to view and send voice messages using a browser from any device with a web browser.

Mitel has made every attempt possible to ensure that the MiCollab AM web client is compatible with browsers that support HTML5, and standard JavaScript, but results in such browsers may vary. Currently, the MiCollab AM web client supports the following web browsers:

- Apple Safari®
- Google Chrome
- Microsoft Edge
- Microsoft Internet Explorer® (Versions 11 and above)
- Mozilla Firefox®

MiCollab AM Web Client Features

The MiCollab AM web client, optimized for web browsers in both desktop and mobile environments, provides a convenient navigation menu pane that allows subscribers quick and easy access to their message folders.

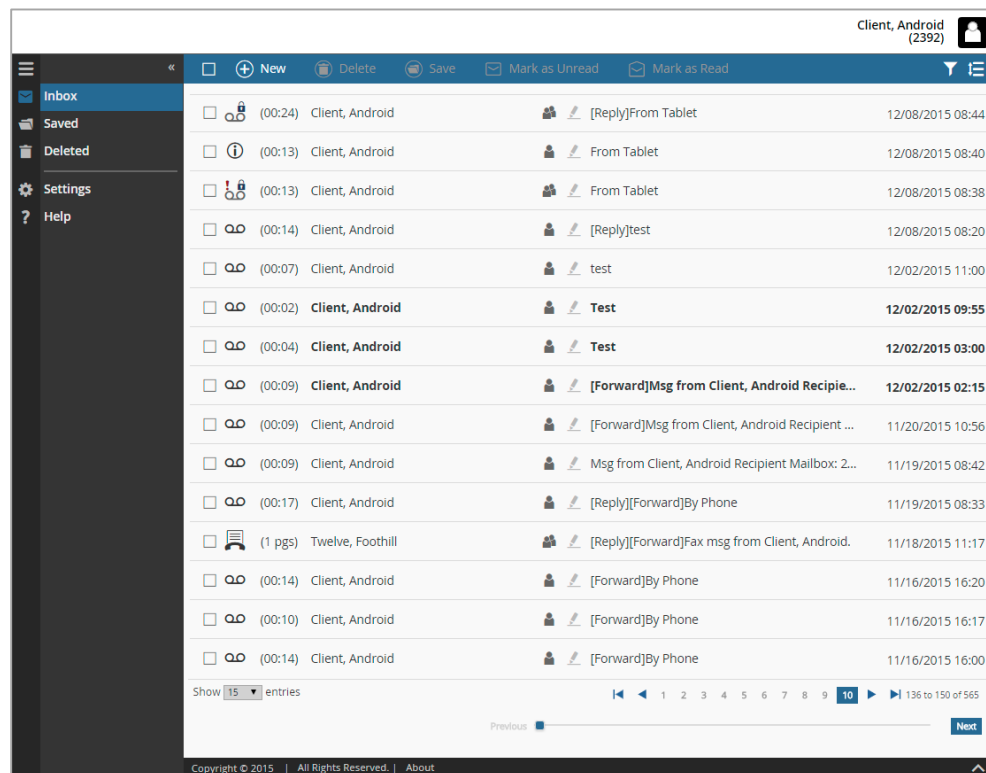


Figure 1. MiCollab AM Web Client Layout

Using the MiCollab AM web client, subscribers can perform the following tasks:

- Send voice messages.
- Listen to voice messages, reply to them, and forward them.
- View fax messages, reply to them (with a voice message), and forward them (with a voice annotation if RightFax is integrated with the MiCollab AM system).
- Play, view, save, or delete voice and fax messages.

The message folders, **Inbox**, **Saved**, and **Deleted**, allow the subscriber to review saved messages and recover messages awaiting deletion.

Depending on the environments, subscribers can select one of the following methods for recording and listening to voice messages:

- **Telephone** requires a subscriber to configure the web client with a telephone number that MiCollab AM can reach by dialing. When a subscriber clicks the **Record** button to send a voice message or clicks the **Play** button for message playback, MiCollab AM dials the telephone number specified in **Settings**. Then the subscriber can pick up the phone when it rings and record or listen to the message.
- **Microphone/Speakers** deliver the recording and listening capabilities directly on the web browser. Microphone allows subscribers to directly record their voice message through the supported web browsers. Speakers allow subscribers to listen to voice messages through the web browsers.

NOTE The voice recording functionality is available only through the Chrome, Edge, and Firefox browsers.

How It Works

The MiCollab AM web client 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 the web client, 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, the web client enables you to encrypt these transactions using Secure Sockets Layer (SSL) on the web server.

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. The MiCollab AM web client does not include a certificate. You must purchase and install a certificate to use SSL.

Acquiring a SSL 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.

Message Cache Manager

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

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

NOTE Message Cache Manager is not a required component of the MiCollab AM web client. However, it is recommended that you use Message Cache Manager to optimize System Server performance.

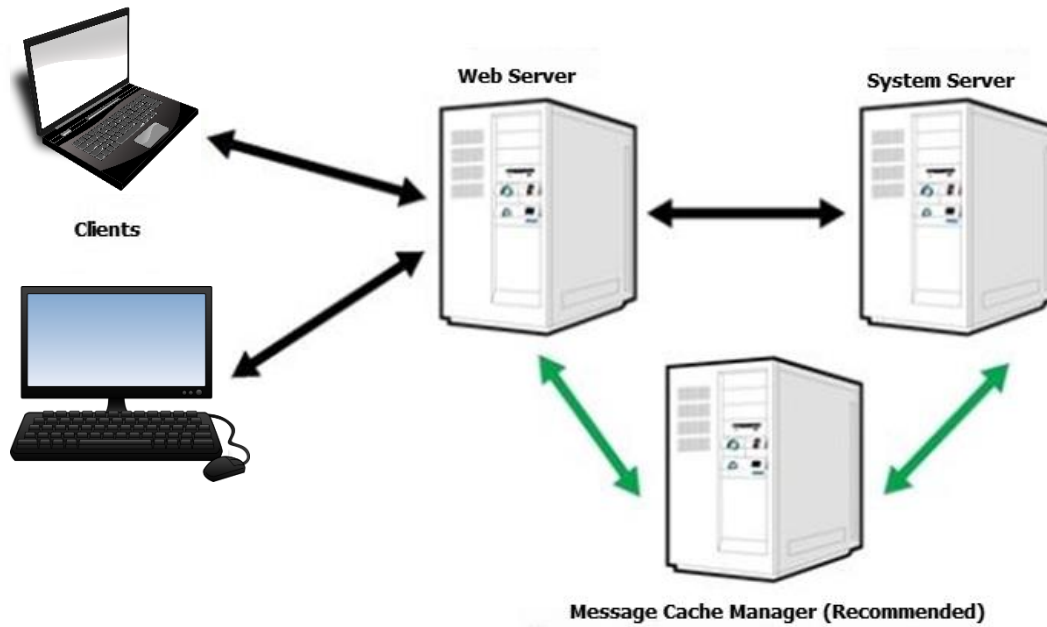


Figure 2. Web Client, MiCollab AM, and (optional) Message Cache Manager

Before Installing the MiCollab AM Web Client

This section lists the installation requirements for successfully installing the MiCollab AM web client. 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.

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)
- The MiCollab AM web client 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 2008 R2 with Service Pack 1 or Windows Server 2012 R2 with the Windows Internet Information Server (IIS) version 6.x, 7.0, 7.5 or 8.x component installed
- World Wide Web Publishing Service installed and running
- PHP versions 5.6.x 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 2008 R2 with Service Pack 1 or Windows Server 2012 R2
- Apache Web Server versions 2.2.x or above
- PHP versions 5.6.x 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 versions 5.6.x 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 or USB drive (for software installation)

Message Cache Manager Server Requirements

- Windows Server 2008 R2 with Service Pack 1 or Windows Server 2012 R2
- 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 the MiCollab AM web client can access the Message Cache Manager Server.
- Message Cache Manager can run on the same server platform as the MiCollab AM web client, 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 the web client. For more information, refer to the [Configuring Subscriber's Web Browsers](#) section. The following are the minimum requirements for client workstations running the web client:

- Compatible web browser (refer to the [What is the MiCollab AM Web Client?](#) Section).
- Connection to the local area network (LAN) or to the World Wide Web via an Internet Service Provider (ISP).
- A telephone or microphone/speakers to record or listen to voice messages.
- A fax viewer capable of displaying multiple-page TIFF documents, such as the OpenText RightFax Viewer, the Microsoft Windows Picture and Fax Viewer, or Apple Preview for Mac.

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.

Installing the MiCollab AM Web Client

Regardless of which server platform you choose to host the MiCollab AM web client – 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 client software.

Installing the 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.

NOTE PHP version 5.6.x can be installed using the Windows Platform installer from Microsoft.

For the MiCollab AM web client-specific configuration instructions, refer to the [Installing the PHP Interpreter](#) section.

Configuring IIS

Before you configure IIS, add a folder to the **\inetpub\wwwroot** folder on your web server. Name the new folder *WebClient*. It becomes the root folder for the MiCollab AM web client web site.

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 Web sites is 80, but adjacent port numbers such as 75 or 82 also work.
- In the list of starting page names for the default web site, 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 client address (URL).
- After you have set up IIS, create a new web site using the **\inetpub\wwwroot\WebClient** folder as the home directory.
- You may also want to create a test web site 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 web sites 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 the MiCollab AM web client. 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 the MiCollab AM web client.

NOTE

1. 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.

2. PHP version 5.6.x can be installed using the Windows Platform installer from Microsoft. Otherwise, PHP need to be configured manually.

Creating Working Folders in the PHP Directory

After you have installed the PHP software, create two new folders and name them *Upload* and *Session* within the directory where you installed PHP. During the MiCollab AM web client 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

1. You do not need to edit the PHP.ini file on a Windows 2008 R2 with Service Pack 1 or 2012 R2 platform. Under Linux, editing of the PHP.ini file varies with each distribution and build.
2. If the PHP version has changed from PHP 5.3.x (or lower) to 5.4.x, the PHP.ini will need to be updated to include upload/session folder location information.

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 the MiCollab AM web client 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 Step 7.

- 7 Exit your web browser.

Changing the Permissions of the Configuration Directory

Upon initial configuration of your MiCollab AM Mobile Admin server, you must make the *config*, *logs*, and *temp* directories on your web server writable to the web server's guest account. As such, you need to update the permission of the **config**, **logs**, and **temp** folders to give full control to 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 client 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 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)
Windows 2008 R2 with Server Pack 1 IIS 7.x	Grant Full Control permissions to the default Internet Guest Account on the web server platform (USER_platformname)(IIS7 account is IUSR)
Linux	Use the <code>chmod</code> and <code>chown</code> 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 the web client to function correctly.

Table 9. Port configuration purpose

Port	Purpose
80	Primary HTTP port for the web client 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 the MiCollab AM web client on an IIS server, you must go back to IIS Administration and start the web client now.

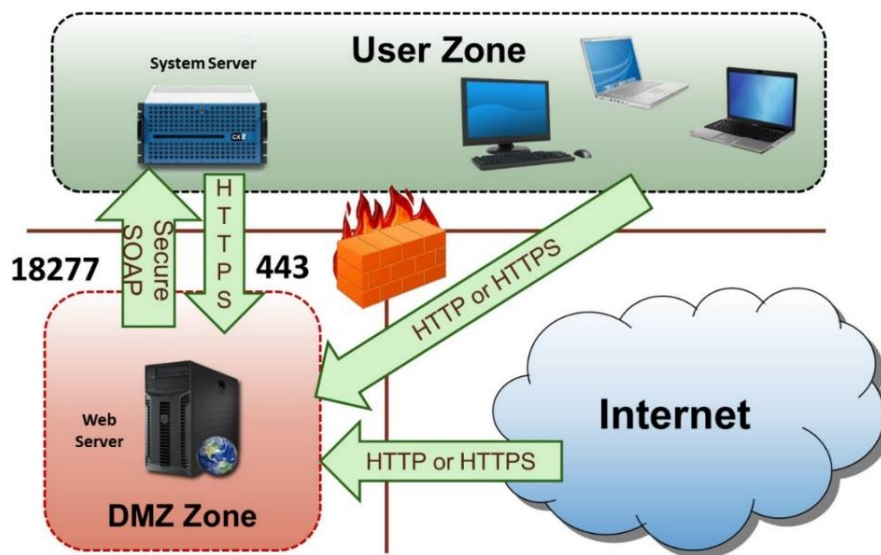


Figure 3. Firewall Setup Diagram

Installing the MiCollab AM Web Client

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

To install the MiCollab AM web client 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 displays. 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\Web Client** folder on the installation media.

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

Configuring the MiCollab AM Web Client

Once you have installed the web client 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 client settings.

NOTE For additional configuration options, see [Appendix A – Configuring the MiCollab AM Web Client with an XML/Text Editor](#).

Configuring Server Settings

The administrator must configure the encryption type and the network location of the MiCollab AM System Server and Message Cache Manager server (if used) in order for the MiCollab AM web client to communicate properly with the System Server and Message Cache Manager server.



NOTE If you are using the web client to access multiple MiCollab AM System Servers, you must identify all System Server addresses in the **Server List** section.

To configure server settings:

- 1 Launch your web browser and access the **admin.php** file for the MiCollab AM web client.
The default address is **http://servername/webclient/webclient/admin.php** where **servername** is the network name or domain name of your web client.
- 2 On the sign in page, sign in using your administrator login credentials.
- 3 Under **Server Settings**, configure the following options:

Table 11. MiCollab AM Server Settings Options

Server Settings Option	Description
Encryption Type	Select the type of encryption to use by the web client when communicating with the System Server and Message Cache Manager. <ul style="list-style-type: none">• Select HTTP to enable encryption. (Default Type)• Select HTTPS if you want to use an added encryption layer of SSL/TLS. <div>IMPORTANT Failing to set the encryption type explicitly on the configuration page can cause connections to fail after an upgrade.</div>

Message Cache Manager Address	Enter the IP address or the FQDN of the Message Cache Manager server.
Server Display Name	Enter the name of your MiCollab AM System Server.
Server Address	Enter the IP address or FQDN of your MiCollab AM System Server.
Save Icon 	Click the Save icon to save the server information. Clicking the Save icon also inserts a new line for more servers.
Trash Icon 	Click the Trash icon to remove the corresponding server.

Changing the Logo Image

The logo image generally represents the branding of the web client application. The administrator should make sure that your company's logo image is correctly uploaded and displayed at the upper left corner of the web client prior to making the web client available to the subscribers.

To upload/change a logo image:

- 1 Launch your web browser and access the **admin.php** file for the MiCollab AM web client.
The default address is **http://servername/webclient/webclient/admin.php** where **servername** is the network name or domain name of your web client.
- 2 On the sign in page, sign in using your administrator login credentials.
- 3 In **Logo Image** under **Application Settings**, select **Upload new image**.
- 4 Click the **Choose File** button and locate the logo image file you want to use.
The preview of the selected logo image is displayed.
- 5 Click **Save**.

Linking a URL to Logo

If you have uploaded your company's logo image, you can link your company's website or any other URL to the logo so the subscribers can click and open the corresponding web page.

To link a URL to the logo image:

- 1 Launch your web browser and access the **admin.php** file for the MiCollab AM web client.
The default address is **http://servername/webclient/webclient/admin.php** where **servername** is the network name or domain name of your web client.
- 2 On the sign in page, sign in using your administrator login credentials.
- 3 In **Home Page** under **Application Settings**, select the **Link home page URL to logo** checkbox.

- 4 In the text field, type the URL.
- 5 Select an option to open the web page in new page or in the current page.
- 6 Click **Save**.

Changing the Application Name

The default name for the web client is usually MiCollab AM or the name of the system. The administrator can change the name of the application to meet your company's branding policy.

To change the application name:

- 1 Launch your web browser and access the **admin.php** file for the MiCollab AM web client.
The default address is **http://servername/webclient/webclient/admin.php** where **servername** is the network name of domain name of your web client.
- 2 On the sign in page, sign in using your administrator login credentials.
- 3 In **Application Name** under **Application Settings**, select **Customize**.
- 4 In the text field, type the name of the application.
- 5 Click **Save**.

Configuring Time Format

The administrator can change the format in which message arrival times are displayed to either 12-hour format indicated with AM/PM (06:30 PM) or 24-hour format (18:30) in the message folders.

NOTE Subscribers also can change their own time format individually through their account.

To change time format:

- 1 Launch your web browser and access the **admin.php** file for the MiCollab AM web client.
The default address is **http://servername/webclient/webclient/admin.php** where **servername** is the network name of domain name of your web client.
- 2 On the sign in page, sign in using your administrator login credentials.
- 3 In **Time Format** under **Application Settings**, select the time format preference.
- 4 Click **Save**.

Removing or Renaming the admin.php File for Added Security

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

IMPORTANT The **admin.php** file can pose a security risk to your web client 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 the MiCollab AM web client, you must also configure the Message Cache Manager Server's address in the web client configuration. The easiest way to configure this server address is from the **admin.php** web page. (Refer to the [Configuring Server Settings](#) section for instructions.) 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 Subscriber's Web Browsers

Provide subscribers with the following information to ensure they can use the MiCollab AM web client successfully:

- The web address (URL) of where they can log on to the MiCollab AM web client.

For example,

http://domain/webclient

where **domain** is the domain name you assigned to the MiCollab AM web client web server.

- The required browser settings listed in the following table:

Table 12. Browser Settings

Browser Type	Settings
Internet Explorer	<ul style="list-style-type: none">• Allow cookies• Enable Active Scripting
Chrome, Edge, Firefox, and Safari	<ul style="list-style-type: none">• Allow/Enable cookies• Enable JavaScript

- Optionally, if you make the MiCollab AM web client URL accessible from outside the organization, your subscribers can use the web client 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 the MiCollab AM web client and System Server. It reduces traffic between the MiCollab AM web client and 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 the web client, 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 client 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 MiCollab AM web client server experiences
- How many web client 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.

Server Requirements for Message Cache Manager

The server requirements for Message Cache Manager are:

- Windows Server 2008 R2 with Service Pack 1 or Windows Server 2012 R2
- 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 the MiCollab AM web client can establish communication.
- The firewall must also allow port 18277 for SSL communication on the SOAP server.

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 13. Autorun Options

If autorun is...	Then...
Enabled	<ul style="list-style-type: none">① In the Server Components area, select Message Cache Manager.② The Install Shield Wizard for Message Cache Manager displays.
Not Enabled	<ul 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 displays.

- 5 Click **Next**. The **License Agreement** dialog box displays.
- 6 Click **Yes** to accept the license agreement. The **Choose Destination** dialog box displays.
- 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 displays.
- 8 Click **Next**. The installation starts. When finished, the **Message Cache Manager Initialization** dialog box displays.

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.

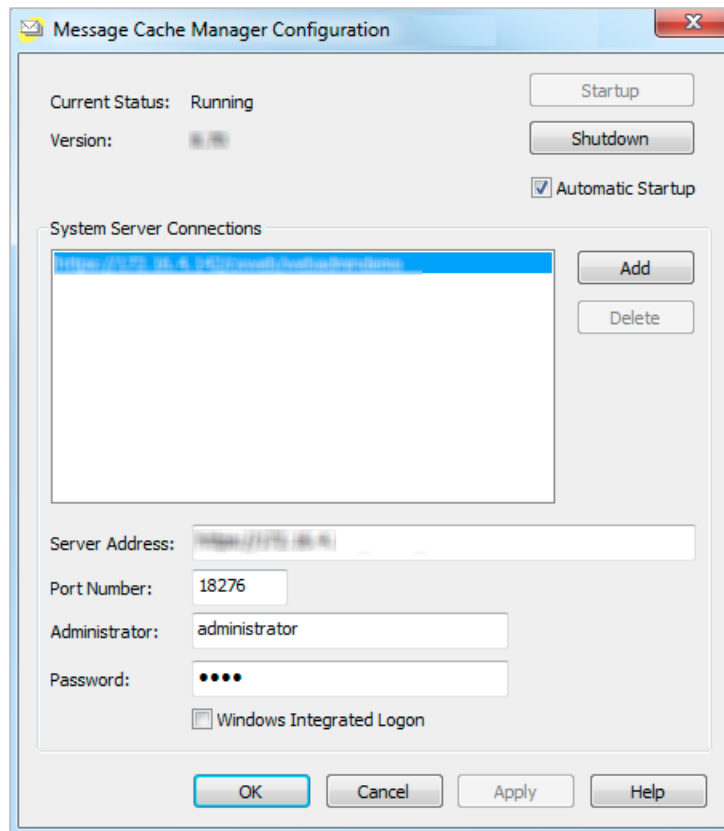
- 12 Click **Next**. The **Install Shield Wizard** dialog box displays.
- 13 Click **Finish**. The installation is complete.

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 displays.



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

Table 14. Message Cache Manager Configuration Utility 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.
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 the MiCollab AM Web Client for Message Cache Manager

Once Message Cache Manager is running, you must configure the MiCollab AM web client to communicate with it. There are two ways you can modify the web client configuration.

- Log on to the MiCollab AM web client and open the **admin.php** file.

In the **Message Cache Manager Address** field, enter the Message Cache Manager Server's FQDN or IP address. (Refer to the [Configuring Server Settings](#) section for more detailed instructions.)

Follow the steps in [Appendix A – Configuring the MiCollab AM Web Client with an XML/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 the MiCollab AM web client to communicate with the Message Cache Manager server, you can start Message Cache Manager.

To start Message Cache Manager:

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

Appendix A – Configuring the MiCollab AM Web Client with an XML/Text Editor

You can modify the MiCollab AM web client 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.

NOTE 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 the MiCollab AM web client 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 client 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:

```
<server name="SERVER_NAME">edit only here</server>
```

NOTE Not all of the settings shown in the example below may be available in your system.

```
<?xml version="1.0"?>
<!DOCTYPE WPMConfig SYSTEM "config.dtd">
<wpmconfig>
  <servers>
    <message_cache_manager></message_cache_manager>
    <server name=""></server>
    <soap_protocol>https</soap_protocol>
    <cxxml_namespace>http://www.avstgroup.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_flash_player>1</allow_flash_player>
    <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>1</refresh_list>
    <default_playback>flash</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>
    <recaptcha_public_key></recaptcha_public_key>
    <recaptcha_private_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>
    <saml_idp_target_url></saml_idp_target_url>
    <saml_idp_metadata_url/>
    <saml_certificate></saml_certificate>
    <saml_assertion_url></saml_assertion_url>
    <saml_app_identifier></saml_app_identifier>
    <webservices_userid></webservices_userid>
    <allow_call_alert_mobile>1</allow_call_alert_mobile>
    <enable_call_screening_non_mobile>1</enable_call_screening_non_mobile>
    <log_level>off</log_level>
    <company_url></company_url>
    <company_url_open_tab>1</company_url_open_tab>
    <company_logo_path></company_logo_path>
    <product_name></product_name>
    <time_format>24</time_format>
    <web_server_https_port></web_server_https_port>
</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 15. Web client config.xml - Servers

Tag	Attribute Name and Tag Value
<message_cache_manager>	<p>Enter the FQDN or the IP address of the Message Cache Server.</p> <p>For example,</p> <pre><message_cache_manager>192.168.1.125</message_c ache_manager></pre>
<server name="">	<p>Enter the System Server name that you want the MiCollab AM web client 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> <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:</p> <p>The following tags would allow users to select one of two System Servers to log on to their mailboxes:</p> <pre><server name="Seattle">sea.domain.com</server> <server name="San Francisco">sf.domain.com </server></pre>
<soap_protocol>	<p>Enter the transmission protocol. The two options are http (default) and https. Https enables SSL encryption to the SOAP server.</p> <p>For example,</p> <pre><soap_protocol>https</soap_protocol></pre>
<cxxml_name_space>	<p>The URL of the XSL namespace definition for the MiCollab AM web client (currently www.mitel.com)</p> <p>IMPORTANT Do not modify this value.</p>

- 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 16. Web Client Config.xml Application

Tag	Attribute Name and Tag Value
<allow_save_login>	<p>Enable or disable the ability of login persistence to subscribers. This feature allows web client to preserve the context in which subscribers are working when they exit their browsers. The next time the subscribers log in, the web client picks up where it left off with them.</p> <ul style="list-style-type: none"> • 1 or TRUE: (Default) Activate the feature • 0 (default) or any other value: Deactivate the feature <p>NOTE When this feature is active, a subscriber must select the Keep me signed in box on the sign in page to use it.</p> <p>For example: <allow_save_login>1</allow_save_login></p>
<save_login_days>	<p>Enter the number of days that a subscriber's login information persists. The default is two days.</p> <p>For example: <save_login_days>2</save_login_days></p>
<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 the MiCollab AM web client using SSL (Secure Socket Layer).</p> <ul style="list-style-type: none"> • 1 or TRUE: Activate the feature • 0 (Default) or any other value: Deactivate the feature <p>For example: <secure_cookie_only>0</secure_cookie_only></p> <p>NOTE If the MiCollab AM web client site is not using SSL or HTTPS, do not enable the Secure Cookie Flag. Subscribers are unable to access the</p>

	MiCollab AM web client if this flag is enabled and you are not using SSL.
<company_url>	<p>The URL to open if user clicks on the logo.</p> <p>NOTE The URL should be in a full address format including protocol.</p> <p>For example: <company_url>http://www.companydomain.com</company_url></p>
<company_url_open_tab>	<p>Set whether the configured URL for the logo should open in a new tab or in the same tab.</p> <ul style="list-style-type: none"> • 1 : (Default) Open in a new tab • 0 : Open in the same tab <p>For example: <company_url_open_tab>1</company_url_open_tab></p>
<product_name>	<p>Change the name of the application if different from the default name or to meet your company's branding policy. The default name is usually the name of the product.</p> <p>For example: <product_name>Web Client</product_name></p>
<time_format>	<p>Set the default format of the message arrival time displayed in subscriber's message folders.</p> <p>NOTE Subscribers can also change their own time format through Settings as well.</p> <ul style="list-style-type: none"> • 12: 12-hour format • 24: (Default) 24-hour format <p>For example: <time_format>24</time_format></p>

4 Save the file.

Appendix B – Upgrading the MiCollab AM Web Client

Upgrading the MiCollab AM web client 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 the web client that you have made such as logo replacements will be lost as part of this upgrade. Any customizations must be manually applied after the upgrade.

To upgrade your web client system:

- 1 Browse to your web client 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.
- 4 Copy the directory structure of the MiCollab AM web client directories to the existing web folders, overwriting any existing files.
- 5 Copy the **config.xml** file retained as part of the backup to the **config** folder and overwrite the existing file.
- 6 Configure the web client.

Settings configured in the previous version of the web client will be retained via **config.xml**. However, you will need to configure any features not available in the previous version.