

MiCollab Advanced Messaging Web Client Administration Guide

For version 9.0 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 2017, Mitel Networks Corporation

All rights reserved

Contents

Preface	4
References	4
Documentation	4
Documentation Updates	5
Help	5
Document Conventions	5
Frequently Used Terms	6
What is the MiCollab AM Web Client?	7
MiCollab AM Web Client Features	7
How It Works	8
Secure Sockets Layer (SSL) and Certificates	8
Message Cache Manager	9
Before Installing the MiCollab AM Web Client	11
Web Server Installation Requirements	11
Site Requirements	11
Message Cache Manager Server Requirements	11
Workstation Installation Requirements	11
Configuring the Firewall	12
Installing the MiCollab AM Web Client	14
Configuring the MiCollab AM Web Client	18
Configuring Server Settings	18
Configuring Application Settings	19
Configuring Subscriber's Web Browsers	22
Installing Message Cache Manager	23
Configuring Message Cache Manager	24
Configuring the MiCollab AM Web Client for Message Cache Manager	26
Starting Message Cache Manager	26

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 9.0 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: See the *System Installation and Configuration 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 10 and above)
- Mozilla Firefox®
- Opera™

NOTE Depending on the system configuration, you may be automatically logged out of the web client after a period of time. You must re-enter your password to continue using the web client.

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.

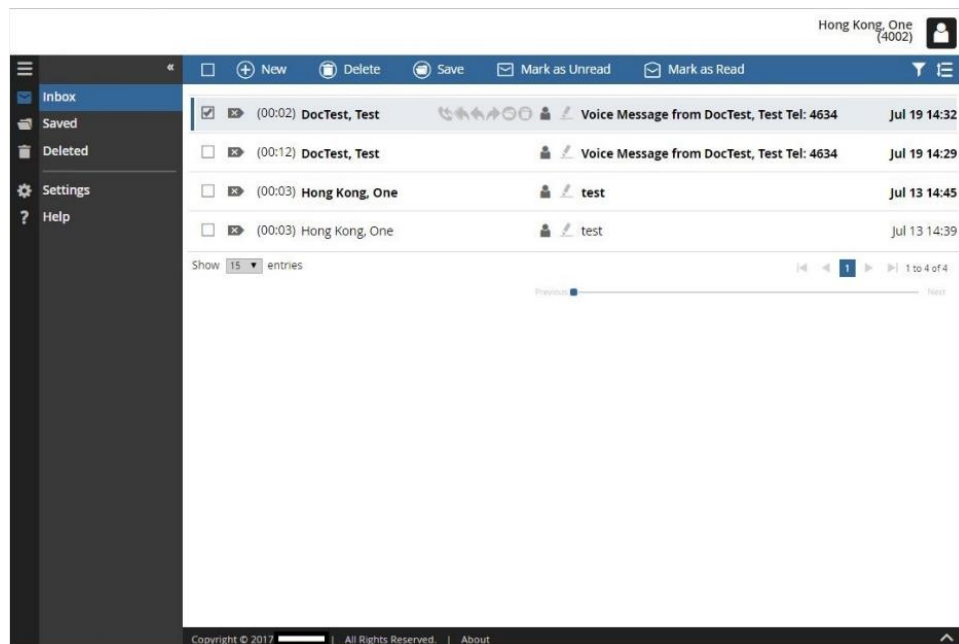


Figure 1. MiCollab AM Web Client Layout

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 following browsers: Safari v11 and above, Chrome, Opera, Edge, and Firefox.

How It Works

The MiCollab AM web client 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.

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 The web client depends on the Message Cache Manager to get messages for logged on users. For a single tenanted system, the MiCollab AM system SOAP server acts as a Message Cache Manager, and therefore a separate standalone Message Cache Manager is not required for the web client. However, to correctly configure a multi-tenanted system with the web client, a separate standalone Message Cache Manager is required that targets that server from within the web client.

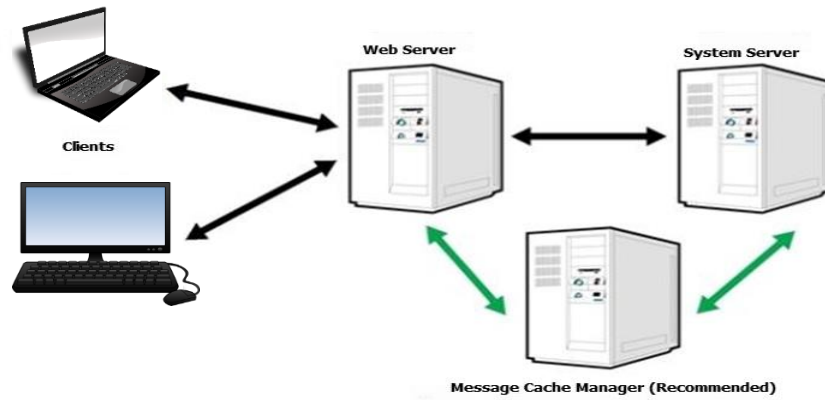


Figure 2. Web Client, MiCollab AM, and Message Cache Manager (required for a multi-tenanted system)

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

Message Cache Manager Server Requirements

- Windows Server 2008 R2 with Service Pack 1, Windows Server 2012 R2, or Windows Server 2016 (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 the MiCollab AM web client can access the Message Cache Manager Server.
- The firewall must also allow port 18277 for SSL communication on the SOAP 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 XMediusFAX 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.

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 2. 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.

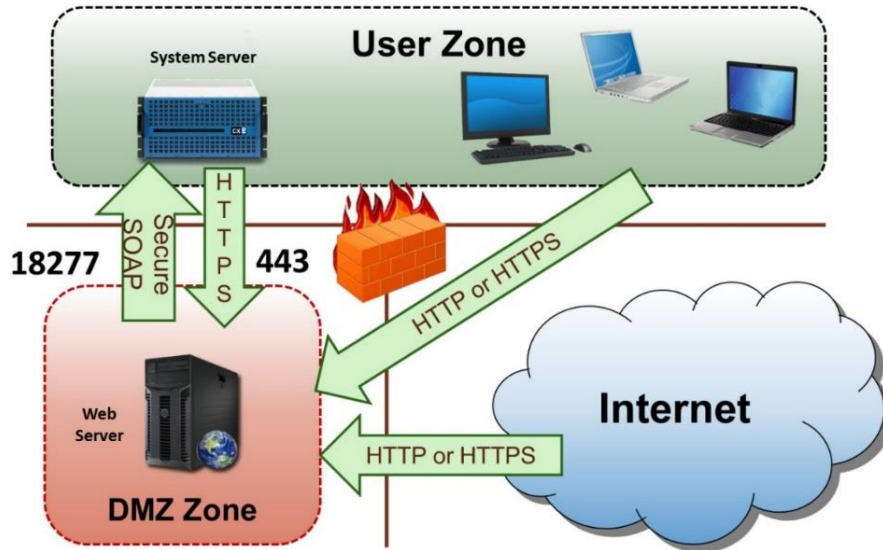


Figure 3. Firewall Setup Diagram

Installing the MiCollab AM Web Client

Mitel has designed the MiCollab AM web client to run on the AngularJS/Node.js platform; thus, there is an option to install the web client when you install MiCollab AM. Updates occur when you update MiCollab AM. For information on how to install MiCollab AM, see the *System Installation and Configuration Guide*.

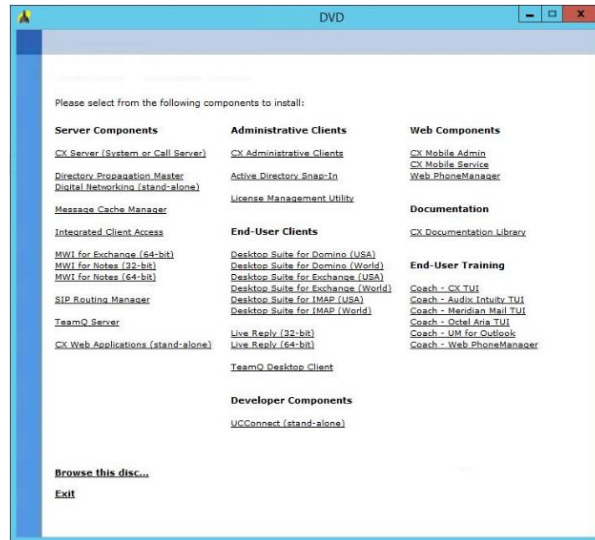
You can also perform a stand-alone installation using either Windows, Linux, or Darwin operating systems.

To install the MiCollab AM web client via the stand-alone installation:

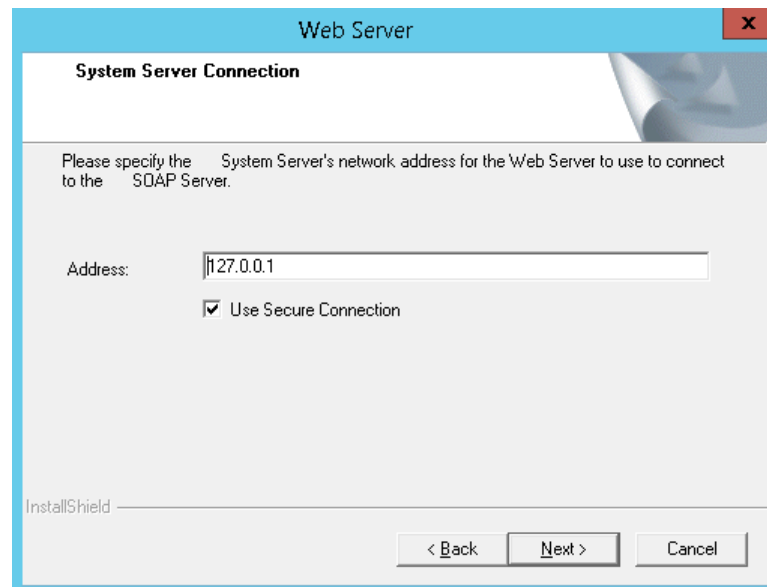
- 1 Log on to the platform using a Windows Administrator account.
- 2 Insert the MiCollab AM Installation Media into the appropriate drive.
- 3 Do one of the following.

Table 3. Autorun Options

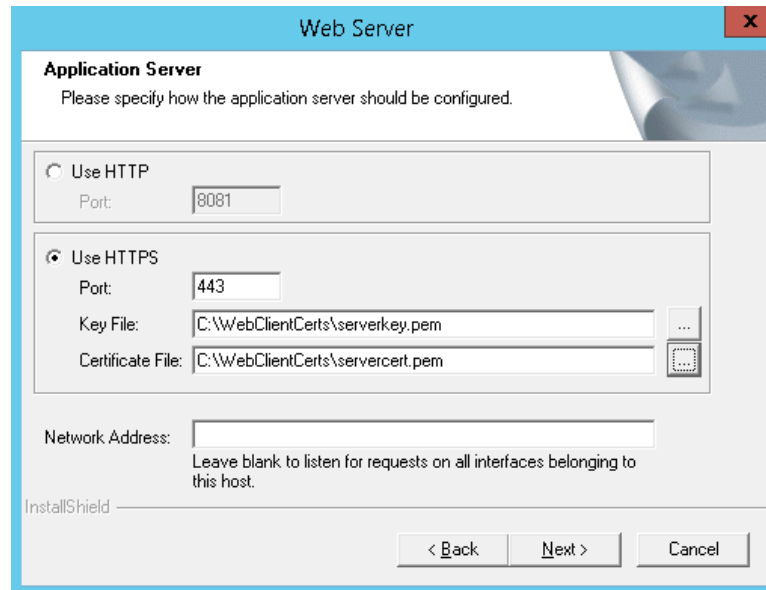
If autorun is...	Then...
Enabled	The MiCollab AM Installation Media menu appears. In the MiCollab AM Server Components area, click MiCollab AM Web Applications (stand-alone) , and then follow the installation instructions on the setup wizard.
Not Enabled	<ol style="list-style-type: none">1. Double-click the start.hta file. The MiCollab AM Installation Media menu appears.2. In the MiCollab AM Server Components area, click MiCollab AM Web Applications (stand-alone), and then follow the installation instructions on the setup wizard.



- 4 In the **Choose Destination Location** dialog box, specify the installation path or accept the default.
- 5 If you are installing the MiCollab AM web client for the first time, proceed with **Step 6**. If you are upgrading the MiCollab AM web client, skip to **Step 11**.
- 6 In the **MiCollab AM System Server Connection** dialog box, specify the location of the MiCollab AM System Server in the **Address** field. By default, the **Use Secure Connection** box is selected. This enables a secured connection between the MiCollab AM System Server and the Web Server.



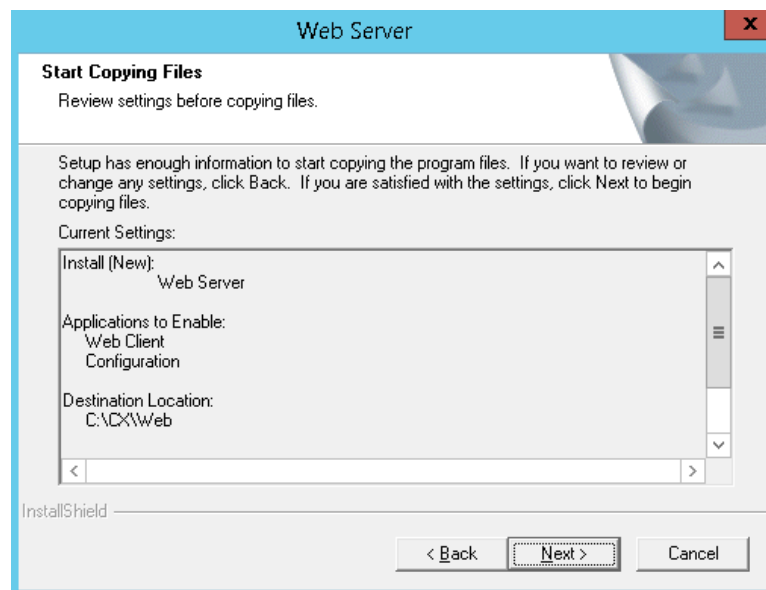
- 7 Click **Next**. The **Application Server** dialog box appears.



- 8 In the **Application Server** dialog box, choose the connection and the port.
 - a If you choose **Use HTTP**, specify the **Port** or accept the default (8081 is standard protocol).
 - b If you choose **Use HTTPS**, specify the **Port** or accept the default (443 is standard protocol) and then enter the location of the **Key File** and **Certificate File** or click the **Browse** button to search for *.pem files.

NOTE The **Key File** and **Certificate File** require PEM format.

- 9 Leave the **Network Address** field blank, or, if you want to specify a different network address, enter the address you want to use to connect to it.
- 10 Click **Next**. The **Start Copying Files** dialog box appears.



- 11 Click **Next**. The Web Client installation begins.

- 12 Click **Finish** to complete the setup and exit the setup wizard.
- 13 Continue to the next section.

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.

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.

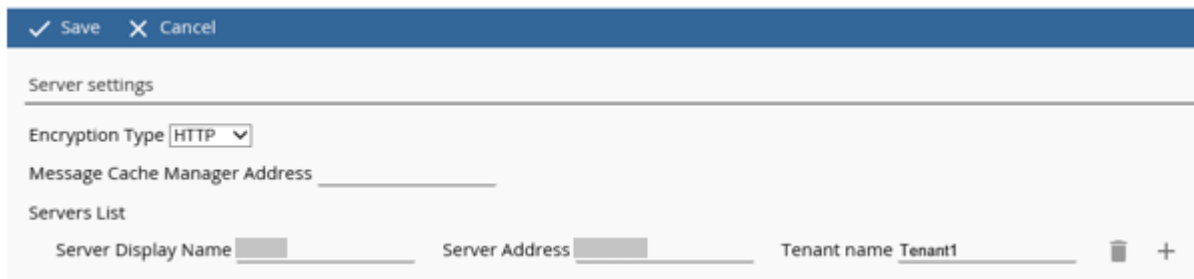
To configure server settings:

- 1 Launch your web browser and enter the web address (URL) for the web client configuration application.

The default address is **http://servername/config-app** 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.




The **Settings – Web Configuration Application** appears.



The screenshot shows the 'Settings – Web Configuration Application' interface. At the top, there is a blue header bar with '✓ Save' and '✗ Cancel' buttons. Below the header, the 'Server settings' section is visible. It includes a dropdown menu for 'Encryption Type' set to 'HTTP'. Below that is a text input field for 'Message Cache Manager Address'. The 'Servers List' section contains a table with columns for 'Server Display Name', 'Server Address', and 'Tenant name'. The first row shows 'Tenant1' in the 'Tenant name' column. There are also trash and add (+) icons at the end of the row.


- 3 Under **Server Settings**, configure the following options:

Table 4. MiCollab AM Server Settings Options

Server Settings Option	Description
Encryption Type	<p>Select the type of encryption to use by the web client when communicating with the System Server and Message Cache Manager.</p> <ul style="list-style-type: none"> • Select HTTP to enable encryption. • Select HTTPS if you want to use an added encryption layer of SSL/TLS. (Default Type)
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.
Tenant name	Enter the name of the Tenant.
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.
Add Icon 	Click the Add icon to add another Server and Tenant to the Servers List .

Configuring Application Settings

The administrator can configure the settings for the web client application prior to making the web client available to the subscribers.

NOTE You must click the **Save** icon  after configuring the application settings for the changes to take effect.

To configure application settings:

- 1 Launch your web browser and enter the web address (URL) for the web client configuration application.
- 2 The default address is **http://servername/config-app** where servername is the network name of domain name of your web client.

- 3 On the sign in page, sign in using your administrator login credentials. The **Settings – Web Configuration Application** appears.

Application settings

Logo image

☒ Use default image

☐ Upload new image

For light background

Choose file

For dark background

Choose file

Home page

☒ Link home page URL to logo

☒ Secure transport

☒ Open in new tab

☐ Open in current tab

Application name

☒ Use default - Web Client

☐ Customize

Product name

☒ Use default -

☐ Customize

Time format

☐ 12-hour format (02:00 PM)

☒ 24-hour format (1400 hours)

Remember me on this computer

☐ Allow remember me

Days to remember me

Security Code Reset Request

☐ Show Security Code Reset Link

reCAPTCHA API Public Key

reCAPTCHA API Private Key

Inactivity Timeout

Logon instruction and information

Additional logon information

- 4 Under **Application Settings**, configure the following options:

Table 5. MiCollab AM Application Settings Options

Application Settings Option	Description
Logo image	Select the company's logo image, which will be displayed in the upper left corner of the web client. <ul style="list-style-type: none">• Select Use default image if you want to use the default image.• Select Upload new image if you want to upload a new image. Click the Choose File button and locate the logo image file you want to use. The preview of the selected logo image is displayed.
Logon instruction and information	Enter customized logon instructions and information prior to making the web client available to the subscribers. Any information entered here will appear on the web client Logon screen.

Additional logon information	<p>Enter additional logon information prior to making the web client available to the subscribers.</p> <p>Any information entered here will appear on the web client Logon screen.</p>
Home page	<p>Select the Link home page URL to logo checkbox to link your company's website or any other URL to the logo so the subscribers can click and open the corresponding web page.</p> <p>Type the URL in the Secure Transport field.</p> <ul style="list-style-type: none"> • Select Open in new tab to open the web page in new page. • Select Open in current tab to open the web page in the current page.
Application name	<p>Select Use default name to use the default name of the web client.</p> <p>Select Customize, and then type the name of the application to meet your company's branding policy.</p>
Product name	<p>Select Use default name to use the default name of the product.</p> <p>Select Customize, and then type the name of the product to meet your company's branding policy.</p>
Time format	Select the time format preference.
Remember me on this computer	Select Allow remember me , and then type the number of days in the Days to remember me field.
Security Code Reset Request	<p>Select Show Security Code Reset Link to enable the Security Code Reset request button on the web client.</p> <p>Type the keys in the reCAPTCHA API Public Key and the reCAPTCHA APT Private Key fields.</p>
Inactivity Timeout	Type the number of minutes the web client can be idle (no user interaction) in background mode or in foreground mode and then locked, before the user must re-authenticate to resume using the web client.

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/user
where **domain** is the domain name you assigned to the MiCollab AM web client web server.
- The required browser settings are listed in the following table:

Table 6. 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.

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 7. Autorun Options

If autorun is...	Then...
Enabled	In the Server Components area, select Message Cache Manager . 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.

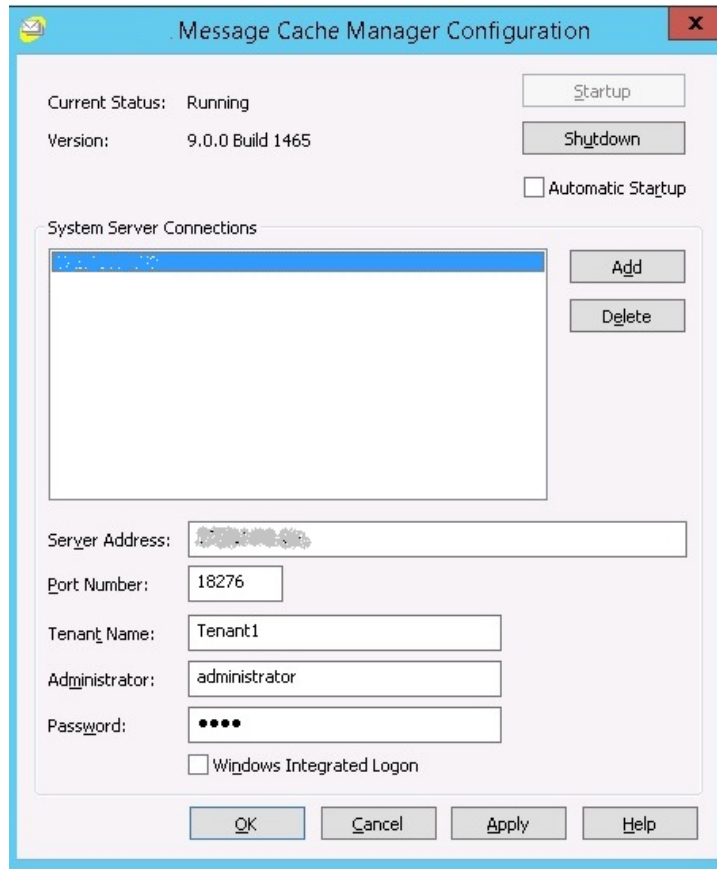
- 12 Click **Next**. The **Install Shield Wizard** dialog box appears.
- 13 Click **Finish**. The installation is complete.

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 8. 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.
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 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 configuration using the config-app.

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.)

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:

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