

# MiCollab Advanced Messaging 23.2

## Web Server

### System Administrator Guide

For version 23.2 and above

## Notice

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

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

## Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto: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 2023, Mitel Networks Corporation

All rights reserved

# Contents

<b>Preface</b>	<b>5</b>
References	5
Documentation	5
Documentation Updates	6
Help	6
Document Conventions	6
Frequently Used Terms	7
<b>What is the MiCollab AM Web Client?</b>	<b>8</b>
MiCollab AM Web Client Features	8
How It Works	10
Secure Sockets Layer (SSL) and Certificates	10
Message Cache Manager	11
<b>Before Installing the MiCollab AM Web Client</b>	<b>12</b>
Web Server Installation Requirements	12
Site Requirements	12
Message Cache Manager Server Requirements	12
Workstation Installation Requirements	12
Configuring the Firewall	13
<b>Installing the MiCollab AM Web Client</b>	<b>15</b>
<b>Configuring the MiCollab AM Web Client</b>	<b>18</b>
Configuring Server Settings	18
Configuring Google reCAPTCHA™	20
Configuring Application Settings	20
<b>Configuring Subscriber's Web Browsers</b>	<b>27</b>
<b>Profile Settings</b>	<b>28</b>
<b>Configuring Call List</b>	<b>29</b>
<b>Configuring Contacts</b>	<b>30</b>
<b>Configuring Preferences</b>	<b>31</b>

<b>Configuring Recordings</b>	<b>32</b>
<b>Configuring Devices</b>	<b>33</b>
<b>Configuring Playback Settings</b>	<b>34</b>
<b>Configuring Notifications</b>	<b>35</b>
<b>Configuring Availability</b>	<b>36</b>
<b>Installing Message Cache Manager</b>	<b>37</b>
Configuring Message Cache Manager	38
Configuring the MiCollab AM Web Client for Message Cache Manager	40
Starting Message Cache Manager	41
<b>OpenText Directory Services (OTDS) Integration</b>	<b>42</b>
OTDS Configuration	42
Create and configure a Resource within OTDS	42
AD Synchronization - Create and configure a Synchronized Partition within OTDS	44
OTDS Connect Web Application Configuration	46
User Sync	47
Group Sync	51
COS Mapping	51
<b>Appendix A – How to Configure Single Sign-On</b>	<b>53</b>
Setting up AD FS to work with CX-E Web Server	53
Setting up MiCollab AM to Support SSO	55
Setting up the Web Server to work with AD FS for SSO	55

# Preface

This guide describes how to install and configure the MiCollab AM web client and the Message Cache Manager.

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

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

To successfully implement the MiCollab AM web client in an organization, the assistance of the following individuals, who constitute the implementation team, is required:

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

**IMPORTANT** Ensure each member of the implementation team receives a copy of this 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 MiCollab AM Documentation Library includes the following documents and resources:

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

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

## Documentation Updates

Documentation updates may be available from the following sources:

- Mitel-certified technicians can view or download documents and program files from our partner web site: [www.mitel.com](http://www.mitel.com)

## Help

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

## Document Conventions

The following conventions are used in this document:

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

Example: **Enter**

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

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

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

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

- **User Interface (UI) Element Names.** Names of UI elements such as dialog boxes, windows, screens, menu items, tabs, buttons, and icons are shown in bold.

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

- **User Input.** Information required to be typed is shown in italics.

**Example:** Type the password *voicemail*.

- **Warning, Caution, Important, and Notes.** Text for the contents that require attention are shown as follows:

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

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

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

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

## Frequently Used Terms

Table 1. Frequently Used Terms

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

# What is 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 MiCollab AM web client after a period of time. You must re-enter your password to continue using the MiCollab AM 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.

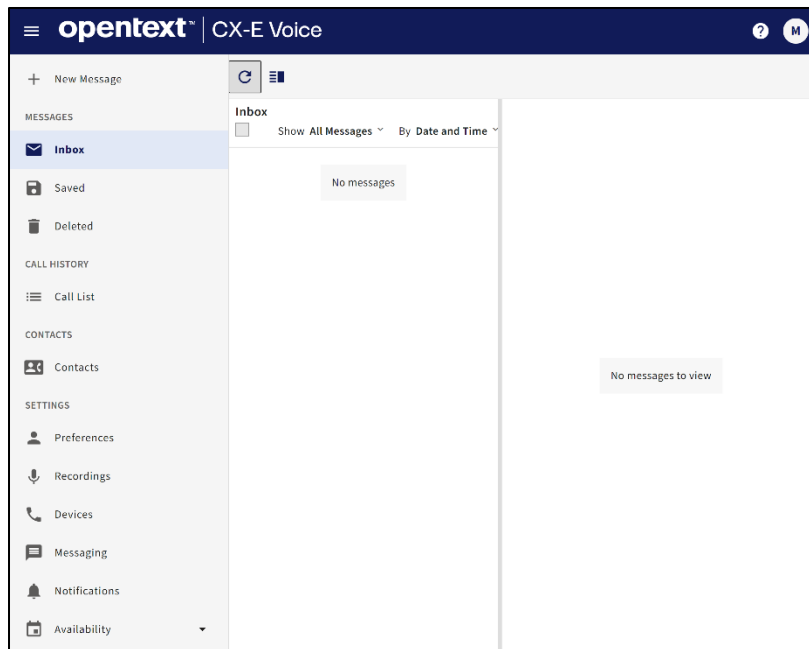


Figure 1. MiCollab AM Web Client Layout

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 XMediusFAX or 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, listening, or viewing voice messages:

- **Phone** requires a subscriber to configure the MiCollab AM 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 **Audio and Call Management** 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.

- **Transcribe Voice Messages.** When enabled you can receive, view, and edit voice message transcriptions in near-real time wherever you have service. Once activated, new incoming messages are transcribed. Transcribed messages continue to display if you toggle the feature off.

**NOTE** This feature is configured by the administrator using the **Let User See and Configure** setting.

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

## 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 MiCollab AM 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 MiCollab AM 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 MiCollab AM web client server and the System Server. It is a transparent application that acts as a liaison between the MiCollab AM web client application and the MiCollab AM System Server. It provides the following features to the MiCollab AM 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 MiCollab AM web client servers.
- Supports multiple System Servers (Digital Networking).
- Multiple Message Cache Manager applications can point to one System Server.

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

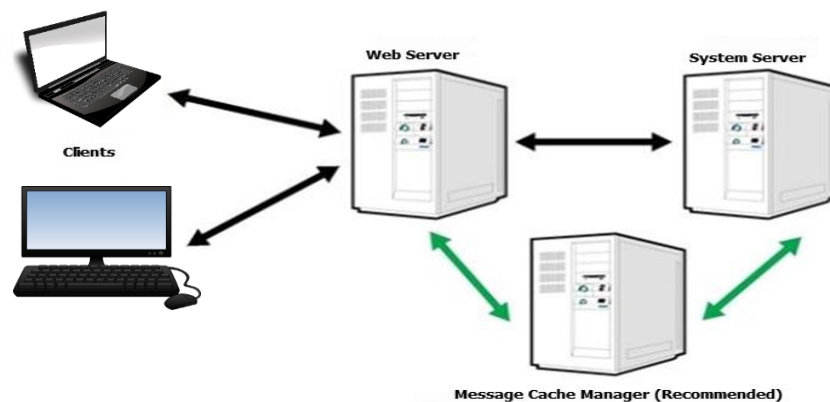


Figure 2. MiCollab AM Web Client, MiCollab AM, and Message Cache Manager (Recommended)

# 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 2012 R2, Windows Server 2016 (Server with Desktop Experience), Windows Server 2019 (Server with Desktop Experience), or Windows Server 2022 (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 MiCollab AM 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 MiCollab AM 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 phone 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 MiCollab AM web client to function correctly.

Table 2. Port Configuration Purposes

Port	Purpose
80	Primary HTTP port for the MiCollab AM web client site
	<b>NOTE</b> 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 MiCollab AM web client now.

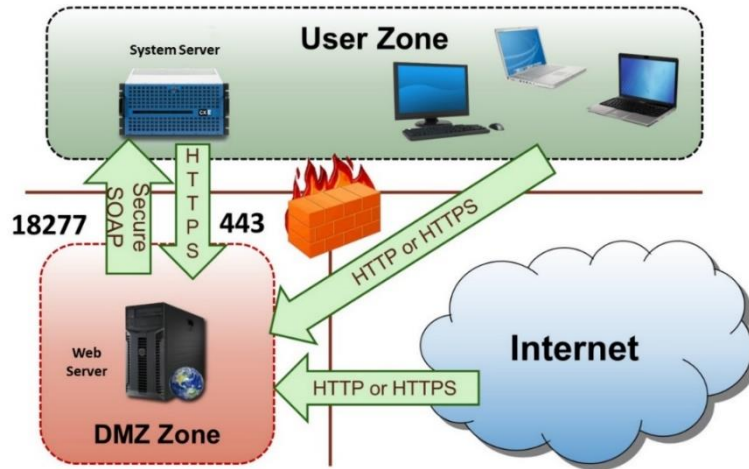


Figure 3. Firewall Setup Diagram

# 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 MiCollab AM 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*.

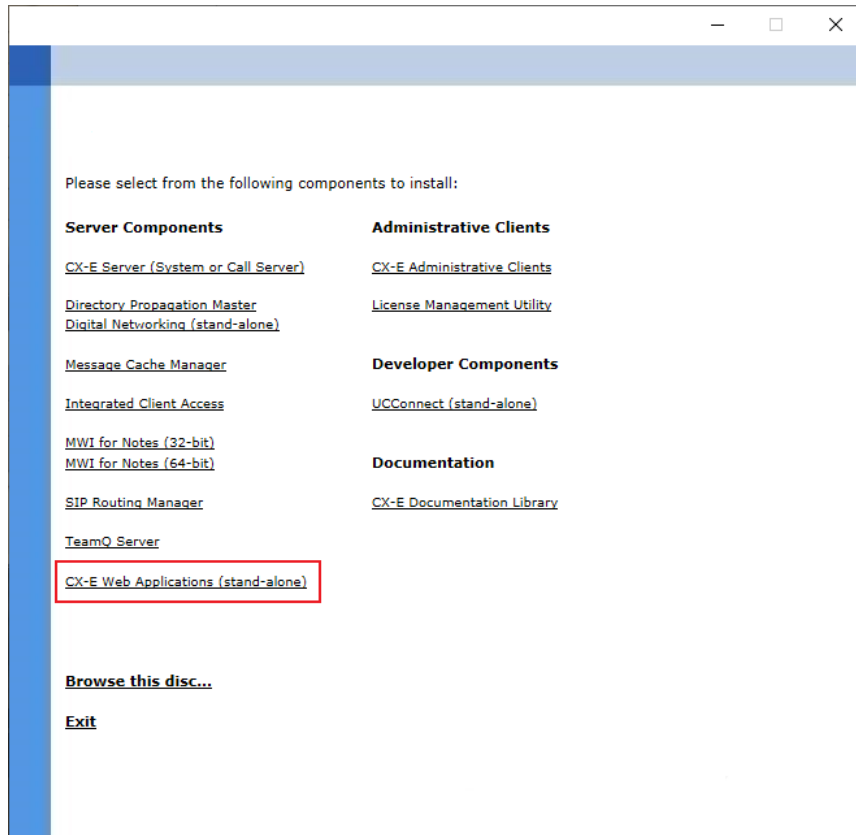
You can also perform a stand-alone installation using either Windows, Linux, or Darwin operating systems.

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

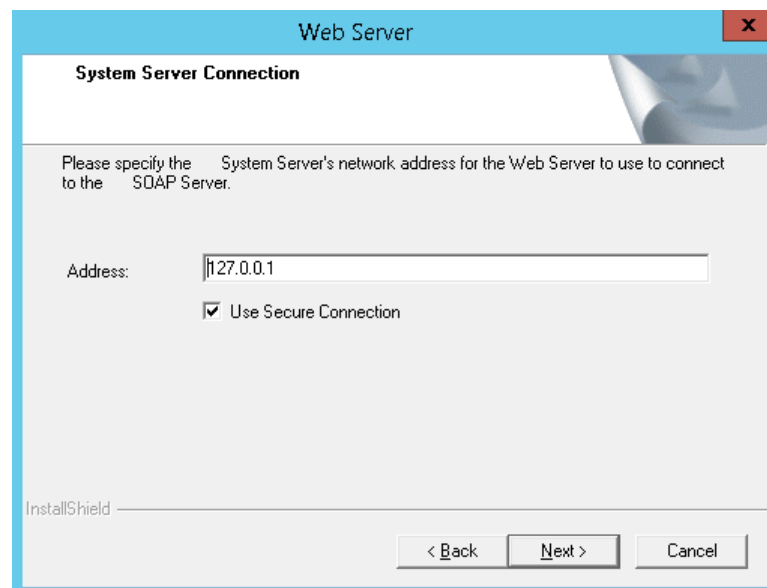
- 1 Log on to the platform using a Windows Administrator account.
- 2 Insert the MiCollab AM Installation Media into the appropriate drive.
- 3 Do one of the following:

Table 3. Autorun Options

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



- 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.

The screenshot shows the 'Web Server' dialog box with the 'Application Server' tab selected. The title bar says 'Web Server' with a close button. The main heading is 'Application Server' with a subtext 'Please specify how the application server should be configured.' Below this, there are two radio button options: 'Use HTTP' (selected) and 'Use HTTPS'. Under 'Use HTTP', there is a 'Port' field with the value '8081'. Under 'Use HTTPS', there is a 'Port' field with the value '443', a 'Key File' field with the path 'C:\WebClientCerts\serverkey.pem', and a 'Certificate File' field with the path 'C:\WebClientCerts\servercert.pem'. Each of these three fields has a browse button (three dots) to its right. Below these fields is a 'Network Address' field, which is currently empty. A note below it says 'Leave blank to listen for requests on all interfaces belonging to this host.' At the bottom left, it says 'InstallShield'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 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.

**IMPORTANT** If you plan to configure Single Sign-On (SSO), you must select **Use HTTPS**. See [Appendix A – How to Configure Single Sign-On](#) for more information.

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

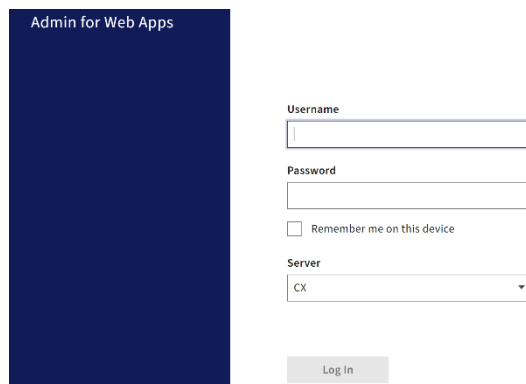
### To configure server settings:

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

The default address is **https://servername/config-app** where **servername** is the network name of domain name of your MiCollab AM web client.

**NOTE** While non-secure (http) access is not recommended, the port number is needed in the address if non-SSL Web Client access is used. For example: **http://servername:8081/config-app**.

The administrator login page for the MiCollab AM web client appears.




Enter your MiCollab AM administrator's Username, Security Code, and Server Address, and then click **Sign in**.

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

2 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 used by the MiCollab AM web client when communicating with the System Server and Message Cache Manager.</p> <ul style="list-style-type: none"> <li>• Select <b>HTTP</b> to enable encryption.</li> <li>• Select <b>HTTPS</b> if you want to use an added encryption layer of SSL/TLS. (Default Type)</li> </ul>
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.
Use for Graph Notification	<p>Select the <b>Use for Graph Notification</b> check box if using the Microsoft Graph API to get message notifications.</p> <p><b>NOTE</b> If there is more than one server, only one check box can be selected at a time.</p>
Save Icon	Click the <b>Save</b> icon to save the server information.
Trash Icon	Click the <b>Trash</b> icon to remove the corresponding server.
Add Icon	Click the <b>Add</b> icon to add another Server and Tenant to the <b>Servers List</b> .

- 3 Click the **Save** icon  after configuring the server settings for the changes to take effect.


## Configuring Google reCAPTCHA™

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

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

## Configuring Application Settings

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

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

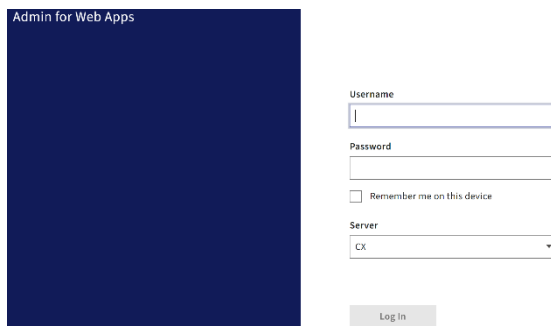
### To configure application settings:

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

The default address is **https://servername/config-app** where **servername** is the network name of domain name of your MiCollab AM web client.

**NOTE** While non-secure (http) access is not recommended, the port number is needed in the address if non-SSL Web Client access is used. For example: **http://servername:8081/config-app**.

The administrator logon page for the MiCollab AM web client appears.



- 2 Type your MiCollab AM administrator's Username, Security Code, and Server Address, and then click **Sign in**.

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

---

### Application Settings

---

#### Logo image

☐ Use default image  
☒ Upload new image

For light background

No file chosenChoose File

For dark background

No file chosenChoose File

#### Home page

☒ Link home page URL to logo

☒ Secure transport

☒ Open in new tab  
☐ Open in current tab

#### Application name

☒ Use default  
☐ Customize

---

#### Product name

☒ Use default  
☐ Customize

#### Time format

☐ 12-hour format (02:00 PM)  
☒ 24-hour format (1400 hours)

#### Voice messages

☐ Users can download and save messages to local computer

#### Remember me on this computer or device

☐ Allow remember me

Days to remember me

2

#### Authorization

reCAPTCHA API Public Key

reCAPTCHA API Private Key

☐ Show security code reset link

☐ Enable reCAPTCHA for security code reset request page

☐ Enable reCAPTCHA for login page

#### Logs

☐ Enable logs for standard Web Client

☐ Enable logs for Exchange Notification web app

Inactivity timeout (minutes)

5

Message refresh interval (seconds)

40

Logon instruction and information

Additional logon information

#### SAML SSO

☐ Enable SAML SSO

##### IDP information

IDP metadata URL

Fetch IDP Information

IDP target URL

IDP certificate

##### SP information

Assertion URL

Application identifier

☒ Enable auth context

Auth context class

urn:oasis:names:tc:SAML:2.0:ac:classes:Password

WebServices UserID

WebServices password

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

Table 5. MiCollab AM Application Settings Options

Application Settings Option	Description
Logo image	<p>Select the company's logo image, which will be displayed in the upper left corner of the MiCollab AM web client.</p> <ul style="list-style-type: none"> <li>• Select <b>Use default image</b> if you want to use the default image.</li> <li>• Select <b>Upload new image</b> if you want to upload a new image, and then click the <b>Choose File</b> button and locate the logo image file you want to use. The preview of the selected logo image is displayed.</li> </ul>
Home page	<p>Select the <b>Link home page URL to logo</b> 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 <b>Secure Transport</b> field.</p> <ul style="list-style-type: none"> <li>• Select <b>Open in new tab</b> to open the web page in new page.</li> <li>• Select <b>Open in current tab</b> to open the web page in the current page.</li> </ul>
Application name	<p>Select the application name, which will be displayed on the MiCollab AM web client logon page.</p> <ul style="list-style-type: none"> <li>• Select <b>Use default</b> to use the default name of the MiCollab AM web client.</li> <li>• Select <b>Customize</b>, and then type the name of the application to meet your company's branding policy.</li> </ul>
Product name	<p>Select the product name, which will be displayed on the MiCollab AM web client logon page and in the upper left corner of the MiCollab AM web client.</p> <ul style="list-style-type: none"> <li>• Select <b>Use default</b> to use the default name of the product.</li> <li>• Select <b>Customize</b>, and then type the name of the product to meet your company's branding policy.</li> </ul>
Time format	Select the time format preference.
Voice messages	Select <b>User can download and save messages to local computer</b> to allow users to download messages in the Inbox, Saved, and Deleted sections to their local server.

Application Settings Option	Description
Remember me on this computer/device	<p>Select to enable the web browser's ability to remember a subscriber's logon information. If enabled, this appears in the form of a <b>Keep me signed in</b> check box on the MiCollab AM web client logon page.</p> <ul style="list-style-type: none"> <li>• Select <b>Allow remember me</b>, and then type the number of days in the <b>Days to remember me</b> field.</li> <li>• Clear <b>Allow remember me</b>, and note that the <b>Days to remember me</b> field is greyed out.</li> </ul>
Authorization	<p>Configure the Authorization settings as required by your company.</p> <ul style="list-style-type: none"> <li>• Type the keys in the <b>reCAPTCHA API Public Key</b> and the <b>reCAPTCHA API Private Key</b> fields.</li> <li>• Select <b>Show Security Code Reset Link</b> to enable the Security Code Reset request feature on the MiCollab AM web client logon page.</li> </ul> <div style="background-color: #e6f2ff; padding: 10px; margin: 10px 0;"> <p><b>NOTE</b> For information on using and configuring the Security Code Reset feature, please see the following topic in the MiCollab AM online help: <i>Configuring the Security Code Reset Feature</i>. In addition, for this feature to work properly, the default SMTP provider in MiCollab AM must be properly configured. Please refer to MiCollab AM documentation for configuration instructions.</p> </div> <ul style="list-style-type: none"> <li>• Select <b>Enable reCAPTCHA for security reset request page</b> to enable the reCAPTCHA human verification test on the Security Request page.</li> <li>• Select <b>Enable reCAPTCHA for login page</b> to display a reCAPTCHA human verification response test on the MiCollab AM web client logon page.</li> </ul>

Application Settings Option	Description
Logs	<p>This setting allows the administrator to enable Web Client specific logging. The logging is disabled by default. If enabled, the logs are located in the logs <a href="#">\\Web\data\logs\</a> folder. The logs are separated in two categories.</p> <ul style="list-style-type: none"> <li>• Select <b>Enable logs for standard Web Client</b> to allow the creation of logs for the following: <b>User</b> (non-server side logs from the client user application), <b>Config-app</b> (non-server side logs from the client config-app application), and <b>Apps</b> (anything not contained in the user or config-app logs – currently only SOAP logs are written).</li> <li>• Select <b>Enable logs for Exchange Notification web log</b> to create logs specific to <b>Exchange-notification</b>. This is specific to when graph notification is enabled.</li> </ul> <p>Logs are named using the log type along with a date-time stamp in the title.</p> <div> <p><b>NOTE</b> Logging is usually enabled as directed by support. Additionally, the settings mentioned only pertain to the log types specified. There is additional logging that occurs automatically.</p> </div>
Inactivity Timeout (Minutes)	<p>Type the number of minutes the MiCollab AM 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 MiCollab AM web client.</p>

Application Settings Option	Description
SAML SSO	<p>Configure the settings related to Security Assertion Markup Language (SAML) Single Sign-On (SSO) as required by your company. These settings are not enabled by default. For more information, see <a href="#">Appendix A – How to Configure Single Sign-On</a>.</p> <ul style="list-style-type: none"> <li>• Select <b>Enable SAML SSO</b> to enable the SSO feature.</li> <li>• Enter the Uniform Resource Locator (URL) for the Identity Provider (IdP) Metadata in the <b>IDP Metadata URL</b> field.</li> <li>• Click <b>Fetch IdP Information</b> to automatically fetch the correct <b>IdP Target URL</b> and <b>IdP Certificate</b> settings.</li> <li>• Enter the <b>Assertion URL</b>.</li> <li>• Enter the <b>Application Identifier</b>.</li> <li>• Select <b>Enable Auth Context</b> to enable the application to send an Authentication Context (AuthContext) request to AD FS.</li> <li>• Enter the <b>WebServices User ID</b>.</li> <li>• Enter the <b>WebServices Password</b>.</li> </ul>
Logon instruction and information	<p>Enter customized logon instructions and information prior to making the MiCollab AM web client available to the subscribers.</p> <p>Any information entered here will appear on the MiCollab AM web client logon page.</p>
Additional logon information	<p>Enter additional logon information prior to making the MiCollab AM web client available to the subscribers.</p> <p>Any information entered here will appear on the MiCollab AM web client logon page.</p>

# 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

**https://domain/user**

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

**NOTE** While non-secure (http) access is not recommended, the port number is needed in the address if non-SSL Web Client access is used. For example: **http://domain:8081/user**.

- The required browser settings for their browser. The required browser settings are listed in the following table:

Table 6. Required Browser Settings

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

- (Optional) Whether or not your subscribers can access the MiCollab AM web client from outside the organization. If you make the MiCollab AM web client URL accessible from outside the organization, your subscribers can use the MiCollab AM web client to keep up-to-date on their messages from anywhere: in the office, at home, and on the road.

# Profile Settings

Using the MiCollab AM 23.2 web client, users can now manage their personal settings. The following sections are available for the user when selecting the avatar profile:

- **Change Security Code** – For changing the password
- **Desktop Notification** – To turn the desktop notification feature on or off. This is used for incoming message notification
- **Audio and Call Management** – To change the phone number or method used to record and play the messages
- **Resources** – To access the training materials or help content provided by the administrator
- **Tell Us What You Think** – To provide feedback about the application
- **Log Out**

# Configuring Call List

MiCollab AM 23.2 provides Web Client users the ability to view and manage their call history. To enable this feature, the system administrator needs to enable the **Personal Assistant license** for the user account in administration.

**NOTE** Call List is the home page for those users who do not get their messages in Web Client.

# Configuring Contacts

With MiCollab AM 23.2 you can provide users the ability to add, modify, and remove contacts so they can personalize their Contacts list. This functionality is available for locally stored contacts only. To enable this feature, the system administrator needs to enable the **Personal Assistant license**, and contacts store location needs to be set to **Local** in the Speech tab for the user account in administration.

**NOTE** The contacts section will not be exposed to the user in Web Client when **Personal Assistant** is not licensed and enabled, or if the contact storage location is set to **External** for the user account.

# Configuring Preferences

MiCollab AM 23.2 provides Web Client users with the ability to manage their presentation, distribution group, call settings, personal assistant settings, transcription setting and voice intercept messaging settings. To enable some of these features, the system administrator must enable the below mentioned settings for the user account in administration:

- **Distribution Group** – Assign a Distribution List to the user. Multiple distribution groups can be assigned to a user.
- **Call Settings** - Enable the **Let user see and configure setting** for the following: Call Screening, Call Blocking (both under Auto Attendant section in the Features tab), and select Call Processor or Busy Call Processor in the ESP section of Answering tab
- **Speech** - Enable the **Let user see and configure setting** in the Speech tab.
- **Personal Settings** – Enable the Personal Assistant license. This includes Use Speech Recognition (for Subscriber Session and Call Completion) and Total Hands Free. This is located in the Speech tab of administration.
- **Embedded Transcription** – Select a service provider and enable the **Let user see and configure setting** under Embedded Voice Message Transcription Service section in the Features tab
- **Voice Intercept Messaging (VIM)** - Enable the **Let user see and configure setting** in the VIM tab

**NOTE** The visibility of these features can be controlled independently for each section.

# Configuring Recordings

MiCollab AM 23.2 allows users to record, review, re-record or delete their recorded name and greetings. Other than the standard greetings, users can also make a recording for availability state greetings when the **Personal Assistant license** and **Availability** feature is enabled by the system administrator.

**NOTE** To allow the user to enable the Out-of-office greeting feature, the system administrator needs to enable the **Let user see and configure setting** in the Answering tab for the user account in administration.

# Configuring Devices

With MiCollab AM 23.2 your users can now self-manage most Web Client settings on the Devices page. This includes adding, editing, and removal. One also has the ability to set primary devices as well as the ability to deactivate the device at which they can be reached.

**NOTE** The extension and shared devices are managed by the administrator.

# Configuring Playback Settings

MiCollab AM 23.2 provides Web Client users with the ability to select and manage their own Message playback settings preferences. These settings can be found in the **Messaging** page under the **Settings** group on the application **Navigation** panel.

**NOTE** The enabled/disabled state of the Listen by type, Play first message automatically, Envelope content when played automatically, and Play envelope automatically input fields are dependent on the TUI type that is set for the user's mailbox.

# Configuring Notifications

MiCollab AM 23.2 provides Web Client users with the ability to configure whether, and when, the system notifies them that a new message has arrived. Users can also set their mailbox to automatically forward messages to another user for new messages that have arrived. To enable these features, the system administrator must enable the below mentioned settings for the user account in administration:

- Email Notification – Enable the Let user see and configure setting under Simple Um in the Email tab
- Text Message Notification (SMS) - Enable the Let user see and configure setting in the SMS tab
- Daily Outcall Notification – Enable the Let user see and configure setting under Daily Message Reminder in the Msg Notification tab
- Immediate Outcall Notification – Enable the Let user see and configure applicable settings in the Msg Notification tab
- Automatic Message Forwarding - Enable the Let user see and configure applicable settings in the Msg Forwarding tab

**NOTE** The visibility of these features can be controlled independently for each section.

# Configuring Availability

MiCollab AM 23.2 provides a user with the ability to enable and manage information about their availability. This includes defining their work hours and availability schedule, as well as allowing for configuring the settings for each availability state. To enable this feature, the system administrator needs to enable the **Personal Assistant license, and** the **Let user see and configure applicable settings** which is located two places in the user account in administration: the Availability Processing section in the Main tab or the Availability tab.

# 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 MiCollab AM 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 MiCollab AM 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 MiCollab AM 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 <b>Message Cache Manager</b> . The <b>Install Shield Wizard for Message Cache Manager</b> appears.

If autorun is...	Then...
Not Enabled	<ol style="list-style-type: none"> <li>1. Go to <b>Start &gt; My Computer</b>, and then double-click the drive where the MiCollab AM Installation Media is inserted.</li> <li>2. Browse to the <b>Server Components</b> area, select <b>Message Cache Manager</b>, and then double-click <b>Setup</b>.</li> <li>3. The <b>Install Shield Wizard for Message Cache Manager</b> appears.</li> </ol>

- 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.

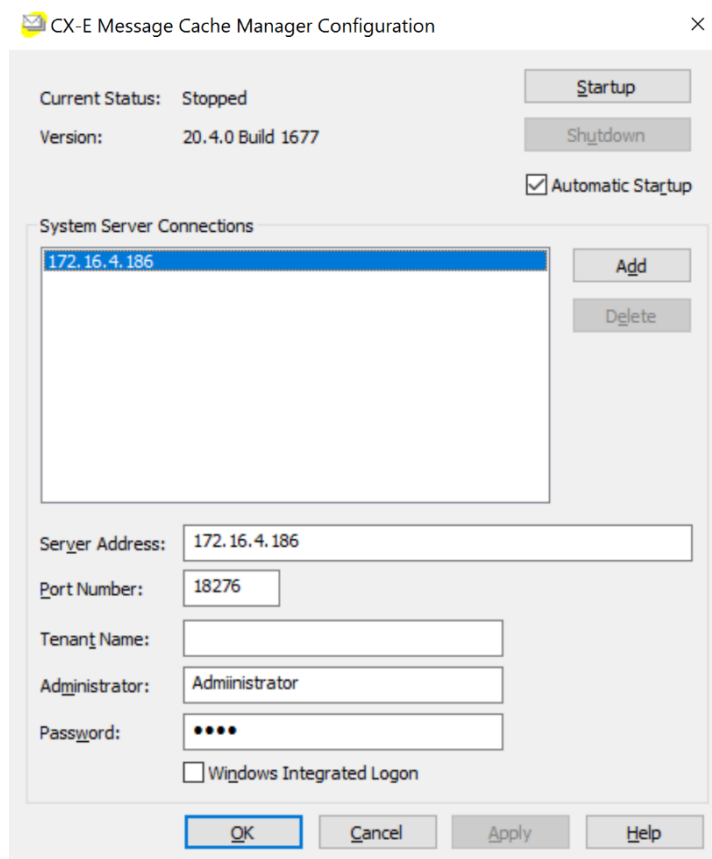
- 12 Click **Next**. The **Install Shield Wizard** dialog box appears.
- 13 Click **Finish**. The installation is complete.

## 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 <b>Startup</b> to start the Message Cache Manager Service.
Shutdown button	Click <b>Shutdown</b> 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.

Field	Description
Add	Click <b>Add</b> to add a System Server to the configuration.
Delete	To remove a System Server from the list, highlight the System Server, and then click <b>Delete</b> . <div> <b>NOTE</b> Only additional System Servers can be deleted; the initial System Server configuration can only be edited. </div>
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	The name of the Tenant.  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 <b>Tenant Name</b> field is mandatory and a Tenant Name must be entered. The <b>Tenant Name</b> is not mandatory for a single tenanted system.
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.

### To configure the MiCollab AM web client for Message Cache Manager:

- 1 Log on to the MiCollab AM web client configuration using the config-app.
- 2 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.

# OpenText Directory Services (OTDS)

## Integration

OpenText Directory Services (OTDS) synchronizes user and group account information, excluding passwords, from an enterprise directory server to an OpenText Enterprise Information Management (EIM) product. An enterprise directory server typically stores identity information (for example users and groups) as well as authentication and authorization information for an enterprise. Supported enterprise directories include Active Directory and select LDAPv3 compliant servers such as Sun One Directory Server, Oracle Directory Server Enterprise Edition, and Novell eDirectory.

A separate license is not required for OTDS. For information about installing and configuring OTDS, see OpenText My Support.

The following sections document the configurations steps for OTDS to sync users and groups data to MiCollab AM:

- OTDS Configuration
- OTDS Connect Web Application Configuration

## OTDS Configuration

There are three separate configuration items within the OTDS configuration section. These are dealt with in the following sub-sections below:

- 1 Create and configure a **Resource** within OTDS
- 2 AD Synchronization - Create and configure a Synchronized Partition within OTDS
- 3 Create and configure an Access Role within OTDS

## Create and configure a Resource within OTDS

- 1 **Resource** represents the MiCollab AM instance that OTDS will sync with. A resource needs to be first created within OTDS so that users and group data can be synchronized with MiCollab AM. While creating the resource, following options need to be configured correctly:

- a **Users and group synchronization** must be selected along with all related synchronization options.
- b **Synchronization connector** should be set to **REST (Generic)**.
- c For the connection info, provide the URL to the OTDS connector web application. Here is an example below:

```
http://examplecxe.opentext.com:8082/otdsconnect
```

- d Configure the Username and Password fields by providing the credentials of a MiCollab AM administrator. To test the URL and the provided Admin credentials, click **Test Connection**.
- e Configure "User Attribute mappings" per the following table:

Table of User Attribute Mappings for a Resource

Resource Attribute	OTDS Attribute	Format
__NAME__	oTExternalID3	%s
_firstName	givenName	%s
_lastName	sn	%s
_displayName	displayName	%s
_mail	mail	%s
_countryCode	c	%s
_department	oTDepartment	%s
_location	physicalDeliveryOfficeName	%s
_homePhone	oTHomePhone	%s
_mobilePhone	oTMobile	%s
_officePhone	oTTelephoneNumber	%s

- f Configure **Group Attribute Mappings** per the following table and save the **Resource**.

Table of Group Attribute Mappings for a Resource

Resource Attribute	OTDS Attribute	Format
__NAME__	cn	%s
_type	oTType	%s

- 2 Once the **Resource** is created, a dialog is displayed which shows the **Resource** identifier which is a GUID. To verify the activation status of the **Resource**, click **Verify Activation**. The **Resource** will need to be activated first before it can be used.
- 3 Activating the **Resource** is done by sending a POST request to the OTDS API URL, which starts with the URL of the OTDS instance and also has the resource identifier GUID in the URL path. This request can be done via cURL by running the following command:

Note that in the following example, "7f418dd2-17f9-422d-b0a9-e284189f6b62" is the **Resource** identifier:

```
curl -X POST
http://devvm002.blvu.avstlabs.local:8080/otdsws/v1/resources/7f418dd2-17f9-422d-b0a9-e284189f6b62/activate
```

This returns a JSON which contains the secret key (secret\_key) which you need to keep a note of::

```
{
  "secret_key": " 892h6dpVt6GccDdeH6+A6w=="
}
```

- 4 The resource is now created and activated.

## AD Synchronization - Create and configure a Synchronized Partition within OTDS

- 1 Follow the steps in OTDS documentation to create a new synchronized partition for your AD. **User Locations** and **Group Locations** are used to restrict the users and groups that will be imported to OTDS and synchronized with the resource. Special setup for MiCollab AM is noted in this section.
- 2 Configure **User Mappings** per the following table.

Table of User Mappings for a Partition

OTDS Attribute	AD Attribute	Format
c	c	%s
cn	cn	%s
co	co	%s
oTDepartment	department	%s
departmentNumber	departmentNumber	%s
description	description	%s
displayName	displayName	%s
oTFacsimileTelephoneNumber	facsimileTelephoneNumber	%s
givenName	givenName	%s
oTHomePhone	homePhone	%s
initials	initials	%s

OTDS Attribute	AD Attribute	Format
l	l	%s
mail	mail	%s
oTMobile	mobile	%s
o	o	%s
physicalDeliveryOfficeName	physicalDeliveryOfficeName	%s
postalCode	postalCode	%s
sn	sn	%s
st	st	%s
street	street	%s
oTStreetAddress	streetAddress	%s
oTTelephoneNumber	telephoneNumber	%s
title	title	%s
oTSAMAccountName	sAMAccountName	%s
ds-pwp-account-disabled	userAccountControl	%s

- 3 Configure “Group Mappings” per the following table.

Table of Group Mappings for a Partition

OTDS Attribute	AD Attribute	Format
cn	cn	%s
description	description	%s
displayName	displayName	%s
oTType	sAMAccountType	%s
oTSAMAccountName	sAMAccountName	%s

- 4 “Resource” represents the MiCollab AM instance that OTDS will sync with. A resource needs to be first created within OTDS so that users and group data can be synchronized with MiCollab AM. While creating the resource, following options need to be configured correctly:

## Create and configure an Access Role within OTDS

- 1 Follow the steps in OTDS documentation to create a new Access Role.
- 2 Under "User Partitions", add the synchronized partition created in the prior section to the Access Role.
- 3 Under "Resources", add the Resource created in the previous section to the Access Role.
- 4 Click on "Include Groups" to include all groups in the synchronization.

## OTDS Connect Web Application Configuration

OTDS connect section in config-app provides the ability to configure settings that are necessary for importing the users from OTDS to MiCollab AM. You can specify the mailbox range that needs be used while synchronizing the user and distribution list mailboxes. One can control the type of users (UM or non-UM) to be created, the number/device that needs to be considered as primary, group and speech assignments, and various other settings through this section. You have provisions to map the security group name coming from OTDS to a COS mailbox number in MiCollab AM.

### Server list

Server display name	Server address	Logon tenant name	<input checked="" type="checkbox"/> Use for Graph Notification	<input checked="" type="checkbox"/> Use for OTDS Connect	
<input type="text" value="AjitVM006"/>	<input type="text" value="127.0.0.1"/>	<input type="text" value="Tenant1"/>			

## Rules for the OTDS connect server selection and setting configuration:

- 1 The server to be used for synchronization can be selected by checking the 'Use for OTDS Connect' checkbox.
- 2 Only a single server can be selected and configured for synchronization with OTDS. To restrict the admin from selecting multiple servers, the "Use for OTDS Connect" checkbox for other servers are disabled. To enable OTDS for a different server, you need to uncheck the previous selection.
- 3 The OTDS Connect section is visible and editable only when the user is logged on to the server that is selected for synchronization with OTDS.
- 4 If the user changes the selected server for OTDS Connect post configuring the settings under OTDS Connect, then all the settings are defaulted on 'Save'.
- 5 The changes to these settings will be retained even when the user is logged on to a server other than the one which is configured for OTDS, unless the user makes any changes to the server parameters like Server Address, Tenant Name and Use for OTDS Connect fields.
- 6 When a server is not configured for OTDS, then the following helper text is displayed: "Not applicable when you are logged in to a server which is not configured to use with OTDS Connect"

# User Sync

This sub-section contains all the settings related to user mailbox that needs to be configured for the one-way synchronization of OTDS to MiCollab AM.

## OTDS Connect

---

### User sync

#### Mailbox range

Start

6100

End

6900

#### Mailbox number selection criteria

Based on extension ▼

☒ Support collisions

#### Primary extension

Office phone ▼

#### Extension length

1 ▼

#### Primary device

Office phone ▼

☐ Use the display name generated by the CX-E Server rule

## 1 Mailbox Range

This setting determines the range in which the user mailboxes will be created on MiCollab AM during the synchronization process.

- **Start** – To specify the starting range for generating mailbox ID. The character limit for this field depends upon the mailbox range supported by MiCollab AM. If MiCollab AM is configured for supporting 4-digit mailbox number, then the value specified here must be exactly of 4 digits. The value provided cannot be greater than the value in 'End' field.
- **End** – To specify the ending range for generating mailbox ID. The character limit for this field depends upon the mailbox range supported by MiCollab AM. If MiCollab AM is configured for supporting 4-digit mailbox number, then the value specified here must be exactly of 4 digits. The value provided cannot be less than the value in 'Start' field.

## 2 Mailbox number selection criteria

- **Based on extension** – If this is selected, the phone number (based on Primary extension setting) of the user coming from OTDS will be used to generate the mailbox ID. If MiCollab AM is configured for supporting 4-digit mailbox number and the phone number has more than 4

digits, then the last four digits of the number will be used as mailbox ID. If the phone number is less than 4 digits, then zeros (0) are prefixed to match the length.  
This is the default selection.

- Pick from range – If this is selected, the range specified in the 'Start' and 'End' fields will be used to generate the mailbox ID. It is mandatory to specify the mailbox range if this option is selected.

- 3 **Support collisions** – This is only applicable when 'Mailbox number selection criteria' is set to 'Based on extension'. When this checkbox is checked and a mailbox number already exists within MiCollab AM that matches with the phone number of a user coming from OTDS, then MiCollab AM will create a mailbox from the range specified in the Start and End fields. If unchecked, then in case of collision the mailbox create operation would fail.

Also, if this is checked, it is mandatory to specify the mailbox range.

Default selection is unchecked.

4 **Primary extension**

This setting determines the phone number coming from OTDS that will be used as the extension device.

- Office phone – If the corresponding phone number is not present in OTDS for a user, then such a user will not be imported into MiCollab AM. If present, the mailbox creation would be successful, and a device of type Extension would be created for that mailbox.  
This is the default selection.
- Home phone - If the corresponding phone number is not present in OTDS for a user, then such a user will not be imported into MiCollab AM. If present, the mailbox creation would be successful, and a device of type Home Number would be created for that mailbox.
- Mobile phone - If the corresponding phone number is not present in OTDS for a user, then such a user will not be imported into MiCollab AM. If present, the mailbox creation would be successful, and a device of type Personal Mobile would be created for that mailbox.

- 5 **Extension length** – This setting is used to truncate the phone number coming from OTDS for the extension device which is based on the 'Primary extension' field. If the primary extension number has more digits than the 'Extension length' value, then only the last digits matching up to the extension length value is considered for the primary extension number.

*Example:* If 'Extension length' value is set as 5 and the phone number of a user coming from OTDS is 98446322, then the primary extension number for that user in MiCollab AM would be 46322.

If the phone number has less digits than the 'Extension length' value, then number is imported as it is.

If 'Extension length' is set to 0, then the phone number will be mapped as it is. No truncation required. Default value is 0.

6 **Primary device**

This setting determines which of these devices is to be considered as the Primary device on the MiCollab AM system.

- Office phone – If the corresponding phone number is present in OTDS for a user, then this would be set as the primary device. Else the selection for 'Primary extension' will be set as primary device. This is the default selection.

- Home phone – If the corresponding phone number is present in OTDS for a user, then this would be set as the primary device. Else the selection for 'Primary extension' will be set as primary device.
- Mobile phone – If the corresponding phone number is present in OTDS for a user, then this would be set as the primary device. Else the selection for 'Primary extension' will be set as primary device.

- 7 **Use the display name generated by the MiCollab AM Server rule** – This setting determines whether the Display Name field for the user should be generated while adding the user to MiCollab AM. If this is checked, then the display name will be generated in the format of the template set in MiCollab AM, and not what is coming from OTDS. If unchecked, display name coming from OTDS will be used as it is.

Default selection is unchecked.

**System locale**

en-US

**Department**

Department

**Office location**

Location

**Unified Messaging type**

Full

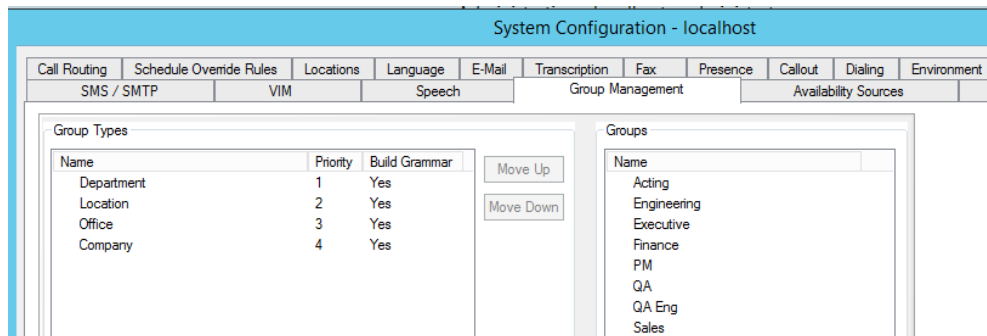
**Email server profile**

Exchange365

☒ Email messages are accessible by phone

- 8 **System locale** – This setting determines the culture to be used for mapping OTDS names to the group names and group type names within MiCollab AM. By default, it is set to "en-US". Contains the list of language sets available for the MiCollab AM system.
- 9 **Department** – This corresponds to the Group Management section in MiCollab AM. Here, you can specify a valid Group Type that exists in MiCollab AM. Users will then be assigned to groups of the specified group type. The department name should be corresponding to the culture that is set via the 'System locale' setting. By default, this is set to "Department". If it doesn't match with the culture that is set or if the department details do not exist within MiCollab AM, the group assignment operation would fail.

Based on the below screenshot, valid values for the 'Department' field would be: Department, Location, Office, Company.



- 10 **Office Location** - This corresponds to the Group Management section in MiCollab AM. Here, you can specify a valid Group Type that exists in MiCollab AM. Users will then be assigned to groups of the specified group type. The location name should be corresponding to the culture that is set via the 'System locale' setting. By default, this is set to "Location". If it doesn't match with the culture that is set or if the location details do not exist within MiCollab AM, the group assignment operation would fail.

Based on the above screenshot, valid values for the 'Location' field would be: Department, Location, Office, Company.

#### 11 **Unified Messaging type**

This setting determines the type of UM profile that will be setup for users.

- None – If this is selected, then all the user mailboxes imported from OTDS will have storage location set as Local (non-UM user) in MiCollab AM. This is the default selection.
- Simple – If this is selected, then all the user mailboxes imported from OTDS will have Simple UM setting checked and an email address specified in 'Email Address' field for the user mailboxes. This will only work if the user has a valid email address coming from OTDS. If a valid email address is not available, then the user won't be imported into MiCollab AM.
- Full – If this is selected, then all the user mailboxes imported from OTDS will have storage location as external store along with other UM settings enabled for the mailbox. This will only work if the user has a valid email address coming from OTDS. If a valid email address is not available, then the user then the user won't be imported into MiCollab AM.

- 12 **Email server profile** –This setting is only enabled when Unified Messaging type is set to Full. It contains a list of all the server profiles configured for MiCollab AM. It is mandatory to select a server profile when enabled. By default, 'None' is selected.

- 13 **Email messages are accessible by phone** – If checked, then the corresponding field in the user mailbox will be checked. If unchecked, then the corresponding field in the user mailbox will remain unchecked. This is only applicable if Unified Messaging type is set to Full and a valid server profile is selected.

Default selection is unchecked.

## Group Sync

This section contains all the distribution list settings that need to be considered for mailbox creation/sync during the one-way synchronization of OTDS to MiCollab AM.

### Group sync

#### Mailbox range

Start

End

#### 1 Mailbox range

This setting determines the range in which distribution list will be created on MiCollab AM during the synchronization process.


- **Start** – To specify the starting range for generating mailbox ID. The character limit for this field depends upon the mailbox range supported by MiCollab AM. If MiCollab AM is configured for supporting 4-digit mailbox number, then the value specified here must be exactly of 4 digits. The value provided cannot be greater than the value in 'End' field.
- **End** - To specify the ending range for generating mailbox ID. The character limit for this field depends upon the mailbox range supported by MiCollab AM. If MiCollab AM is configured for supporting 4-digit mailbox number, then the value specified here must be exactly of 4 digits. The value provided cannot be less than the value in 'Start' field.

**Note:** If the range is not specified, on OTDS sync, the distribution list will not be created on MiCollab AM. The operation would simply fail.

## COS Mapping

This section contains settings to map the Security group name coming from OTDS to a valid COS mailbox number in MiCollab AM. Unlike user and distribution list mailboxes, a COS cannot be created during OTDS sync. Security group name needs to be mapped to an existing COS available in MiCollab AM.

#### Security group to Class of Service (COS) mapping

Security group name	COS mailbox number	
<input type="text"/>	<div>None ▾</div>	<div> </div>

- **Security group name** – The security group name in OTDS needs to be specified here. It must be an exact match or else the sync operation will not be successful.
- **COS mailbox number** – This setting contains the list of all COS MBID's available in MiCollab AM. Map an existing COS mailbox number to the security group name in OTDS. Any members/users added to the security group through OTDS will be reflected in the corresponding COS mailbox in MiCollab AM.  
The default selection is 'None'.

- '+' icon – You can use this icon to add more security group mappings.
- **Bin** icon – You can use this to delete the mappings.

**Note:** You can map different security group name to the same COS mailbox number.

# Appendix A – How to Configure Single Sign-On

The MiCollab AM web server supports Single Sign-On (SSO) using the Security Assertion Markup Language (SAML) protocol with Microsoft Active Directory Federation Services (AD FS). Refer to the following sections for instructions on how to configure AD FS, MiCollab AM, and the MiCollab AM web server for SSO.

**NOTE** For new installations of the MiCollab AM web server, you must choose **Use HTTPS** when you first install. See [Installing the MiCollab AM Web Client](#) for more information.

## Setting up AD FS to work with CX-E Web Server

To set up AD FS to work with the CX-E web server SSO:

- 1 In AD FS Admin, go to **Relying Party Trusts**.
  - Right-click and select Add Relying Party Trust.
  - Choose Claims aware application type and start the wizard.
- 2 When the wizard asks for the option to be used to obtain data, select **Enter data about the relying party manually** and then click **Next**.
- 3 Enter a display name and then click **Next**.
- 4 Skip entering a token encryption certificate and then click **Next**.
- 5 Choose **Enable support for the SAML 2.0 WebSSO protocol** and enter the User SSO service URL.  
Example User SSO service URL:  
**https://domainname/user/saml-logon/complete**
- 6 Click **Next**.
- 7 For the Relying Party identifier, enter a unique name.  
For example:  
You could concatenate the machine name of the MiCollab AM web server and the application name and create an identifier such as **WEBSERVER1-WEB**. You could also let this be a URL such as a URL of the web server machine.
- 8 Click **Add** and then click **Next**.
- 9 For the access control policy, select **Permit everyone**.
- 10 Click **Next**.
- 11 Click **Next** in the **Ready to Add Trust** screen.

- 12 The Relying Party Trust has been created. If you selected the **Configure claims issuance policy for this application** option, you will automatically go into the next step. Otherwise, right-click on the **Relying Party Trust** you just created and choose **Edit Claim Issuance Policy**.
- 13 On the **Issuance Transform Rules** tab, select **Add Rule**.
- 14 Select **Send LDAP Attribute as Claims** as the claim rule template to use and then click **Next**.
- 15 Give the claim a name such as *Get LDAP Attributes*.
  - Attribute Store should be set to Active Directory.
  - LDAP Attribute should be set to E-Mail-Addresses.
  - Outgoing Claim Type should be set to E-mail Address.
- 16 Click **Finish**.
- 17 Once again, select **Add Rule** to add another rule.
- 18 Select **Transform an Incoming Claim** as the claim rule template to use for this rule and then click **Next**.
- 19 Give it a name such as *Email to Name ID*.
  - The incoming claim type should be **E-mail Address** (it must match the **Outgoing Claim Type** configured in rule #1).
  - **Outgoing claim type** is **Name ID** (which maps to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**).
  - **Outgoing name ID** format is **Email**.
- 20 Select **Pass through all claim values** and then click **Finish**.
- 21 Click **OK** to return to the main **AD FS** screen.
- 22 Right-click on the **Relying Party Trust** and choose **Properties**.
- 23 On the **Endpoints** tab, click **Add SAML**.
- 24 Set the following properties for the new endpoint
  - a) The Endpoint type should be **SAML Assertion Consumer**
  - b) The Binding should be **POST**
  - c) Index should be **1**
  - d) Set the Trusted URL to the **Admin SSO service URL** by replacing "user" with "admin" in the URL configured earlier.

**Example Admin SSO Service URL: https://domainname/admin/saml-logon/complete**
- 25 Click **OK**.

# Setting up MiCollab AM to Support SSO

## To set up MiCollab AM to support SSO:

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

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

- 6 Open **MiCollab AM Admin** and configure the e-mail address for each subscriber and administrator that will be using SSO.
  - a) Double-click a subscriber mailbox to open it.
  - b) On the **Main** tab of the subscriber mailbox, in the **E-mail** field, type the same e-mail address that the Identity Provider (IDP) resolves the user to.
  - c) Open the Administrator account.
  - d) In the **E-mail** field, type the same e-mail address that the Identity Provider (IDP) resolves the administrator account to.
- 7 MiCollab AM configuration to support SSO is now complete. Proceed to [Setting up the Web Server to work with AD FS for SSO](#).

# Setting up the Web Server to work with AD FS for SSO

## To configure the MiCollab AM web server for SSO:

- 1 Open the MiCollab AM web server config-app page and log on with the new MiCollab AM administrator account you created in Setting up MiCollab AM to Support SSO.
- 2 In the Application Settings on the web server config-app page, under the SAML SSO section, select Enable SAML SSO.
- 3 Configure the following settings under the **IDP information** group:
  - a) Enter the Uniform Resource Locator (URL) for the Identity Provider (IDP) Metadata in **the IDP metadata URL** field. This URL should come from the system administrator who installed the AD FS service.

- b) Click **Fetch IDP Information** to automatically fetch the correct **IDP target URL** and **IDP certificate** settings.
- 4 The IDP target URL is the URL of the Identity Provider (IDP) Single Sign-on (SSO) service. For AD FS, the URL will typically be something like `https://ADFS_SERVER_NAME/adfs/ls/`
- 5 The IDP certificate is the certificate the IDP uses to sign the SAML assertion. To obtain the certificate from AD FS, open the URL to the metadata of the AD FS service.
- 6 Configure the following settings under the **SP information** group:
- a) Enter the Admin SSO Service URL in the **Admin assertion URL** field. This should exactly match (is case-sensitive too) the URL to the admin page that was configured in AD FS for this Relying Party.
- For example:  
`https://domainname/admin/saml-logon/complete`
- b) Enter the User SSO Service URL in the **User assertion URL** field. This should exactly match (is case-sensitive too) the URL to the user page that was configured in AD FS for this Relying Party.
- For example:  
`https://domainname/user/saml-logon/complete`
- c) Enter the identifier of the application in the **Application identifier** field. This should exactly match (is case-sensitive too) the identifier of the Relying Party that was configured in AD FS.
- d) Select the **Enable auth context** check box to enable the application to send an Authentication Context (AuthContext) request to AD FS. For more information about how AD FS interprets the relative strength of different authentication methods when it evaluates a requested authentication context, refer to the Microsoft Active Directory Federation Services documentation.
- NOTE** The default **Auth Context Class URI** is for the following Authentication Method:  
**Password Protected Transport:**  
`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport.`
- 7 Enter the User ID of the MiCollab AM administrator account that will be used to log on to the SOAP server for creating a user or admin session in the WebServices UserID field.
- 8 Enter the password of the MiCollab AM administrator account that will be used to log on to the SOAP server for creating a user or admin session in the WebServices password field. The password is stored encoded.
- 9 Setting up the Web Server SSO to work with AD FS is now complete. Direct the end user to use the following URL to log in to the MiCollab AM web client: `https://domainname/user/saml-logon/initiate`. The user is first directed to the AD FS server and signs in using their credentials. Then the user is redirected to the MiCollab AM web client sign in page.
- 10 Direct admins to use the following URL to log on to the MiCollab AM web admin: `https://domainname/admin/saml-logon/initiate`.