

MiCollab Advanced Messaging 23.2 Containerized System Deployment and Configuration 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 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

Preface	6
References	6
Documentation	6
Documentation Updates	7
Help	7
Document Conventions	7
Acronyms and Abbreviations	8
Frequently Used Terms	8
Overview	10
Prerequisites	10
Remote Client Applications	10
Deploying MiCollab AM Containers	12
Network Topology	12
Between Containers	12
Cluster Ingress and Egress	12
System Server	12
Volume	12
Hostname	13
MAC Address	13
Memory	13
Network	13
Port Mappings	13
Environment Variables	14
Image	14
Docker deployment example	15
Call Servers	15
Volume	15
Hostname	15
Memory	15
Network	15
Port Mappings	15

Environment Variables	16
Image	16
Docker deployment example	17
Web Client	17
Volume	17
Port Mappings	17
Image	17
Docker deployment example	17
MiCollab AM Media Services	18
Volume	18
Port Mappings	18
Image	18
Docker deployment example	18
Initial System Configuration	19
System Server	19
Call Servers	19
Web Applications	20
Web Client	20
CXMS	21
Upgrading Containers	22
Maintenance Tasks	23
Database Recovery	23
Restoring the backup of the System Server	23
System Server Database Recovery Arguments	23
Restoring the backup of the Call Server	24
Call Server Database Recovery Arguments	24
Call Server Resynchronization	25
Importing a new License	25
Generate and Import a new Self-Signed SSL Certificate	26
Importing a Custom SSL Certificate	26
Resetting an administrator password	26
Resetting the automatic FTPS password	27

Licensing	28
Appendix	29
FTPS for File Copying between Servers	29
External Volumes for Data Persistence	29

Preface

This guide describes how to deploy and perform initial configuration of containerized MiCollab AM.

References

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

Documentation

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

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

Documentation Updates

Documentation updates may be available from the following sources:

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

Help

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

Document Conventions

The following conventions are used in this document:

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

Example: **Enter**

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

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

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

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

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

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

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

Example: Type the password *voicemail*.

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

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

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

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

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

For more related documents, refer to the following list of references:

Table 1. References

Document Type	Document Title
Server Documentation	<i>System Backup and Restore</i>
Server Documentation	<i>System Installation and Configuration Guide</i>
Administration Documentation	<i>Mobile Client Service</i>
Administration Documentation	<i>Web Client</i>

Acronyms and Abbreviations

Table 2. References

Term	Description
FTPS	File Transfer Protocol Secure
SMB	Server Message Block

Frequently Used Terms

Table 3. Frequently Used Terms

Term	Description
System Server	An organization's computer platform(s) that have MiCollab AM software installed and handles the core system functions such as storing messages, database.
Call Server	An organization's computer platforms that have MiCollab AM software installed and serve as the interface to the system (PBX). The Call Server(s)

Term	Description
	interface with the System Server for the purpose of accessing messages, and database.
Container	<p>Somewhat like a Virtual Machine, a container includes a disk image along with an isolated set of processes having a specific role. Containerized MiCollab AM deployments include the following containers:</p> <ul style="list-style-type: none"> • System Server • Call Server • MiCollab AM web client • Web Phone Manager • MiCollab AM Mobile Service
Tenant Administrator Account	<p>Administrator account used by tenants to administer their configuration.</p> <p>The default Tenant Administrator account is 'Administrator' with an empty password.</p>
Site Administrator Account	<p>Administrator account used to configure the site/system and manage tenants but does not have direct access to configure tenant configuration.</p> <p>The Site Administrator account is required when running MiCollab AM Remote System Configuration to configure containerized System Server and any Call Servers</p> <p>The default Site Administrator account is 'SiteAdmin' with an empty password.</p>

Overview

This document explains the unique procedures for deploying and configuring MiCollab AM in a containerized environment, compared to traditional deployments on physical servers and virtual machines. As such, this document does not go into specific orchestration technologies, such as Kubernetes or cloud deployments.

Prerequisites

You must meet the following prerequisites:

- The administrator is knowledgeable in deploying and managing containers in their specific deployment environment and using orchestration technologies of their choice.
- Depending on the configuration requirements, the administrator might need command line/shell access to some of the containers.
- The administrator has access to a server or workstation with a MiCollab AM Client Installation for access to the client applications.
- The administrator has familiarity with the various MiCollab AM products and the traditional installation and configuration methods.
- The administrator has access to the referenced external documents for comprehensive descriptions of the standard installation and configuration tasks.

Remote Client Applications

Traditional installation and configuration of MiCollab AM relies heavily on the usage of the MiCollab AM desktop client applications. Containerized MiCollab AM runs on Windows Server instances without a desktop user interface, so these client applications cannot be run directly on the servers. The solution is to install the MiCollab AM Client Installation on a separate server or workstation, and remotely configure and administer the system.

The following clients are fully supported running remotely:

- MiCollab AM Administration
- MiCollab AM System Configuration
- Reports
- Line Status
- System Status
- Diagnostics

- Mailbox Archive

Keep in mind that a small subset of maintenance tasks cannot be run remotely and must be done using command line utilities directly on the container. For information about command line utilities used with the container, see [Maintenance Tasks](#).

Deploying MiCollab AM Containers

Network Topology

A containerized MiCollab AM environment consists of a System Server container, Call Server containers for scaling, and optional Web application containers. As with a traditional MiCollab AM deployment, these containers must be able to communicate with each other over a network. Some functionality also requires ingress and egress networking outside this set of containers, such as with the PBX or from remote native client applications.

Between Containers

The following routing cases between containers must be supported, ideally using a hostname, otherwise by IP address if the address is static:

- System Server to/from any Call Servers
- Web apps to the System Server

Cluster Ingress and Egress

In the case of Kubernetes, communication between containers is usually automatic, but additional configuration is required to/from the "cluster" of containers, using services and port mapping. Regardless of how the containers are deployed, make sure the following routes are working after the containers are deployed.

- Native clients to the System Server and any Call Servers
- Web browsers to the Web apps
- Call Servers to/from the PBX
- System Server (with call services) to/from the PBX

System Server

The System Server container requires the following arguments when launched. This information applies when you deploy using Docker or Kubernetes.

Volume

To persist data and configuration settings, define a volume mapped to the following location:

```
C:\CX_Volume
```

For more information, see [External Volumes for Data Persistence](#).

Hostname

Specifying a unique hostname for each server can be useful as a routing alternative to using the internal IP address when routing between containers. If not specified, hostnames are auto generated for containers when they are deployed.

NOTE Depending on how the system is licensed, the hostname may be required to have a fixed value, which may require specifying the hostname (using `--hostname`) whenever deploying the container. For more information, see [Licensing](#).

MAC Address

NOTE Depending on how the system is licensed, the MAC address may be required to have a fixed value, which may require specifying a valid MAC address (using `--mac-address`) whenever deploying the container. For more information, see [Licensing](#).

Memory

Depending on the deployment, the container might need to have memory pre-allocated for the container. MiCollab AM System Server and Call Server containers must have at least 8GB of memory.

Network

Specify any necessary network settings, and optionally specify a static IP address.

Port Mappings

The System Server container exposes the following ports:

- TCP 18276 (non-secure SOAP)
- TCP 18277 (secure SOAP)

If the System Server has call services, the following ports are exposed:

- UDP/TCP 5060 (non-secure SIP)
- UDP/TCP 5061 (secure SIP)
- Sets of 10 consecutive UDP ports starting at 10000 *for each telephony line* (RTP)

For example: 10000-10009 (RTP for telephony line 1)
 10010-10019 (RTP for telephony line 2)
 10020-10029 (RTP for telephony line 3)
 10020-10029 (RTP for telephony line 4)
 etc....

Environment Variables

The following environment variables are used to configure the System Server:

Variable Name	Display Name	Notes
ServerRole	Server Role	Required 5 – System Server with call services. 1 – System Server without call services.
ServerAddress	N/A	Optional Defaults to the container's hostname.
SystemName	System Name	Optional Defaults to 'CX-E'.
MbxLength	Mailbox Length	Optional Valid range is 2-15. Defaults to 4.
UseStdDB	Use Standard Database	Optional 1/0. Defaults to 1.
UseSpeechAutoAttendantUI	Auto Attendant User Interface	Optional 1/0. Defaults to 1.
StdDBDirKey	Directory Key Mapping	Optional 1/9. Defaults to 1.
StdDBXferType	Call processor transfer Type	Optional B/M/T for Blind, Monitor, Transfer. Defaults to B.
Location	Location	Optional Defaults to 'Cloud'.

Image

The server image name is `cxevoice-server:23.2`. For more information about the full registry URL from which to pull the server image, contact your MiCollab AM account representative.

Docker deployment example

```
docker run -d --name CXSystemServer --volume CXSystemServerVolume:C:\CX_Volume --hostname CXSystemServer --mac-address CE-78-26-E3-FF-6E --memory=12g -p 18276:18276 -p 18277:18277 -e "ServerRole=1" <image>
```

Call Servers

The Call Server containers require the following arguments when launched. This information applies when you deploy using Docker or Kubernetes.

Volume

To persist data and configuration settings, define a volume mapped to the following location:

```
C:\CX_Volume
```

For more information, see [External Volumes for Data Persistence](#).

Hostname

Specifying a unique hostname for each server can be useful as a routing alternative to using the internal IP address when routing between containers. If not specified, hostnames are auto generated for containers when they are deployed.

Memory

Depending on the deployment, the container may need to have memory pre-allocated for the container. MiCollab AM System Server and Call Server containers must have at least 8GB.

Network

Specify any necessary network settings, and optionally a static IP address.

Port Mappings

The System Server container exposes the following ports:

- TCP 18276 (non-secure SOAP)
- TCP 18277 (secure SOAP)
- UDP/TCP 5060 (non-secure SIP)
- UDP/TCP 5061 (secure SIP)
- Sets of 10 consecutive UDP ports starting at 10000 *for each telephony line* (RTP)

For example: 10000-10009 (RTP for telephony line 1)
 10010-10019 (RTP for telephony line 2)

10020-10029 (RTP for telephony line 3)
10020-10029 (RTP for telephony line 4)
etc....

Environment Variables

The following environment variables are used to configure the Call Server:

Variable Name	Display Name	Description
ServerRole	Server Role	Required Must be set to 4.
TenantID	N/A	Required Must be set to 1.
SystemServerAddress	System Server Network Address	Required FQDN or IP address of the System Server that can be reached by the Call Server.
SystemServerSOAPPort	System Server SOAP Port	Required Must be set to 18276.
AdminUserName	MiCollab AM Administrator	Required Must be a valid Site Administrator account such as 'siteadmin'.
AdminPassword	Password	Required Must be the password for the corresponding Site Administrator account. WARNING Make sure the account is not still at the default empty password, otherwise the Call Server will fail to deploy.

Image

The server image name is *cxevoice-server:23.2*. For more information about the full registry URL from which to pull the server image, contact your MiCollab AM account representative.

Docker deployment example

```
docker run -d --name CXCallServer1 --volume CXCallServer1Volume:C:\CX_Volume --hostname CXCallServer1 --memory=12g -p 18286:18276 -p 18287:18277 -p 5060:5060/udp -p 5061:5061/udp -p 10000:10000/udp -p 10001:10001/udp -p 10002:10002/udp -p 10003:10003/udp -p 10004:10004/udp -p 10005:10005/udp -p 10006:10006/udp -p 10007:10007/udp -p 10008:10008/udp -p 10009:10009/udp -p 10010:10010/udp -p 10011:10011/udp -p 10012:10012/udp -p 10013:10013/udp -p 10014:10014/udp -p 10015:10015/udp -p 10016:10016/udp -p 10017:10017/udp -p 10018:10018/udp -p 10019:10019/udp -p 10020:10020/udp -p 10021:10021/udp -p 10022:10022/udp -p 10023:10023/udp -p 10024:10024/udp -p 10025:10025/udp -p 10026:10026/udp -p 10027:10027/udp -p 10028:10028/udp -p 10029:10029/udp -p 10030:10030/udp -p 10031:10031/udp -p 10032:10032/udp -p 10033:10033/udp -p 10034:10034/udp -p 10035:10035/udp -p 10036:10036/udp -p 10037:10037/udp -p 10038:10038/udp -p 10039:10039/udp -e "ServerRole=4" -e "TenantID=1" -e "SystemServerAddress=CXSystemServer" -e "SystemServerSOAPPot=18276" -e "AdminUserName=siteadmin" -e "AdminPassword=*****" <image>
```

Web Client

The Web Client container requires the following arguments when being launched. This information applies when you deploy using Docker or Kubernetes.

Volume

To persist configuration settings and certificates, define a volume mapped to:

```
C:/CX/Web/data
```

For more information, see [External Volumes for Data Persistence](#).

Port Mappings

The Web Client container exposes the following ports:

- TCP 8081 (HTTP) – *only required if HTTP is desired*
- TCP 443 (HTTPS)

Image

The web client image name is `cxevoice-web:23.2`. For more information about the full registry URL from which to pull the web client image, contact your MiCollab AM account representative.

Docker deployment example

```
docker run -d --name WebClient -p 8081:8081 -p 443:443 --volume WebClientVolume:C:/CX/Web/data <image>
```

MiCollab AM Media Services

The MiCollab AM Media Services container requires the following arguments when being launched. This applies when deploying using Docker or Kubernetes.

Volume

To persist configuration settings, define a volume mapped to:

C:\inetpub\wwwroot\cxms\config

For more information, see [External Volumes for Data Persistence](#).

Port Mappings

The MiCollab AM Media Services container exposes the following ports:

TCP 80 (HTTP)

TCP 443 (HTTPS)

Image

The Media Services image name is *cxevoice-ms:23.2*. For more information about the full registry URL from which to pull the Media Services image, contact your MiCollab AM account representative.

Docker deployment example

```
docker run -d --name CXMS -p 80:80 -p 443:443 --volume  
CXMSVolume:C:\inetpub\wwwroot\cxms\config <image>
```

Initial System Configuration

With traditional MiCollab AM server deployments, database initialization and system configuration are done in a single step using the interactive database initialization wizard in MiCollab AM System Configuration. With containerized MiCollab AM, the database initialization portion is done as part of the deployment process, leaving the licensing and PBX Integration settings configuration. The following describes the system configuration steps for the containerized MiCollab AM servers as well as the web applications.

System Server

After the System Server container has deployed, it will begin the process of configuring the database and doing initial server setup. Monitor the container logs until the container reports the following:

"SOAP Server is running. Connect using System Configuration to configure the system."

To monitor the container logs for this using docker commands, use the following command. Note that the `-f` option does a continual live refresh.

```
docker logs -f <container>
```

NOTE After the container is fully configured, all subsequent Application event log messages will be written to this log for system monitoring.

After setup is complete, use MiCollab AM Remote System Configuration to connect to the container by a routable name or IP address. MiCollab AM Remote System Configuration requires the use of a Site Administrator account, with the system default being 'siteadmin' with an empty password. Note that the password will need to be changed immediately upon the first logon.

MiCollab AM Remote System Configuration will then prompt for the license file. For more information about obtaining a valid license file for this deployment, contact your MiCollab AM account representative. For more information, see [Licensing](#).

If the System Server is configured to have call services (i.e., environment variable `ServerRole=5` was specified), MiCollab AM Remote System Configuration will then present a wizard for telephony configuration of the server.

Finally MiCollab AM Remote System Configuration will be ready and MiCollab AM can be started.

Call Servers

With an initialized System Server, the Call Servers can then be deployed and initialized. After deployment, use the following steps to initialize each Call Server.

After the Call Server container has deployed, it will begin the process of joining the System Server. Monitor the container logs until the container reports the following:

"SOAP Server is running. Connect using System Configuration to configure the system."

To monitor the container logs for this using docker commands, use the following. Note that the -f option does a continual live refresh.

```
docker logs -f <container>
```

NOTE After the container is fully configured, all subsequent Application event log messages will be written to this log for system monitoring.

After setup is complete, use MiCollab AM Remote System Configuration to connect to the container by a routable name or IP address.

MiCollab AM Remote System Configuration requires the use of a Site Administrator account, similar to configuring the System Server. MiCollab AM Remote System Configuration will present a wizard for telephony configuration of the server.

Finally MiCollab AM Remote System Configuration will be ready and MiCollab AM can be started.

Web Applications

The containerized web applications each come pre-installed, requiring only the site-specific configuration to be done. Be sure the System Server is configured and MiCollab AM is running before configuring the web applications.

Web Client

For Web Client, refer to the *Web Client* document. Since much of the installation is already done, refer to the section "Configuring the web Client". For containerized Web Client, the configuration address is <https://servername/config-app> and the user portal is <https://servername/user>.

NOTE Containerized Web Client is set up for both HTTPS and HTTP. HTTPS uses self-signed certificate files by default. To use a custom certificate, refer to the *Web Client* document. Note that the certificate PEM files must be placed in the C:/CX/Web/Data/certs folder.

Note that because the container is deployed without the user interface to configure some optional settings, some edits may need to be made to C:/CX/Web/Config/config.json in the container. This include specifying the Network Address for the service to listen on (versus the default of all interfaces), and a Parent FQDN Server URL.

WARNING Manual modifications to config.json currently are not part of the volume and thus are lost upon redeployment or upgrade.

CXMS

For CXMS, refer to the *Mobile Client Service* document. Since much of the installation is already done, refer to the section "Configuring Mobile Service". For containerized CXMS, the configuration address is <http://servername/cxms/admin.php>.

NOTE In the configuration, the "Reference URL Path" must be modified to be /cxms/cxmns.php.

Upgrading Containers

Instead of installing updates on a container, upgrades occur by pulling a new image and redeploying the container from the new image. Orchestration technologies such as Kubernetes handle this process with minimal downtime, but this can be done using Docker commands as well. The following is the recommended sequence.

Note Be sure to upgrade the System Server before upgrading any Call Server.

Note Before any System Server or Call Server upgrade, it is always recommended to run daily maintenance to create a recent backup of the data.

1. Pull the updated image to a location that can be referenced by Kubernetes or Docker.
2. Stop the running container. Delete the container if the container name is to be re-used.

WARNING Do NOT delete the volume when deleting the container, otherwise all customer configuration and data will be lost.

3. Redeploy the container using the new updated image, referencing the same volume name as the original deployment. This will cause the new container to access the existing customer configuration and data. At this point System Server and Call Server containers will run any necessary database upgrade steps if database changes were made between image versions.

Maintenance Tasks

Database Recovery

For full information on recovering a database backup, refer to the *Recovering a Database* section in the *System Backup and Restore* document.

NOTE Anytime a System Server is restored from backup, all Call Servers will then need to either be resynched or restored from backup.

Restoring the backup of the System Server

To restore a database backup on the System Server, run the following command from CX\Bin:

```
AT_DBAutoCfg.exe /dbrecover=<full path to backup zip file> servername=<override server display name> netaddr=<override network address> init=<1/0> reports=<1/0> recordings=<1/0>
```

NOTE The recovery process takes several minutes, but when successful, will exit with error code 0. If there is an error, the error log can be reviewed at CX_Volume\Log\AT_DBAutoCfg.TSSysInt.log, focusing on the tail end of the log for any details about the error. Technical Support may be required.

System Server Database Recovery Arguments

Field Name	Default	Notes
dbrecover	N/A	Full path to the backup zip file. In containerized MiCollab AM, the online backups will be under C:\CX_Volume\CX_Backups\backup\.
netaddr	Value in backup	Optional override of the IP or DNS address. NOTE Required if the IP address of the container is different from the system where the backup was taken, such as when a database is migrated from one server to another.

servername	Value in backup	Optional override of the Name (Display Name) of the server.
init	0	Set to 1 to completely rebuild the database before restoring. This is generally only needed if the database is being restored onto a new server.
reports	0	Set to 1 to restore the reports from the backup
recordings	0	Set to 1 to restore the messages and other records from the backup

Restoring the backup of the Call Server

NOTE Before restoring a Call Server, the System Server must be online and reachable, however MiCollab AM does not need to be started.

To restore a database backup on a Call Server, run the following command from CX\Bin:

```
AT_DBAutoCfg.exe /dbrecover=<full path to backup zip file> servername=<override server display name> netaddr=<override network address> init=<1/0> reports=<1/0> recordings=<1/0> systemserver_addr=<system server address> systemserver_user=<administrator account> systemserver_pwd=<administrator password>
```

NOTE The recovery process takes several minutes, but when successful, will exit with error code 0. If there is an error, the error log can be reviewed at CX_Volume\Log\AT_DBAutoCfg.TSSysInt.log, focusing on the tail end of the log for any details about the error. Technical Support may be required.

Call Server Database Recovery Arguments

Field Name	Default	Notes
dbrecover	N/A	Full path to the backup zip file. In containerized MiCollab AM, the online backups will be under C:\CX_Volume\CX_Backups\backup\.
netaddr	Value in backup	Optional override of the IP or DNS address. NOTE Required if the IP address of the container is different from the system

		where the backup was taken, such as when a database is migrated from one server to another.
servername	Value in backup	Optional override of the Name (Display Name) of the server.
init	0	Set to 1 to completely rebuild the database before restoring. This is generally only needed if the database is being restored onto a new server.
reports	0	Set to 1 to restore the reports from the backup, otherwise the reports in the current data directory will remain.
recordings	0	Set to 1 to restore the messages and other records from the backup, otherwise the messages in the current data directory will remain.
systemserver_addr	N/A	System Server network address. This address must be reachable by the Call Server.
systemserver_user	N/A	Existing administrator account
systemserver_pwd	N/A	Password for the administrator account

Call Server Resynchronization

In the event of a network failure or after System Server recovery you can resync the Call Server with the System Server. The Call Server must be shutdown to perform resync.

From the Call Server, run the following command from CX\Bin:

```
AT_DBAutoCfg.exe /dbresync
```

Refer to the *System Backup and Restore* document for more information on Call Server Resynchronization.

Importing a new License

In cases where a system needs to be updated with a new license file, use the following steps:

1. Stop the MiCollab AM service.
2. Copy the new license file into the System Server container.

3. Run the following command within the container from CX\Bin:

```
AT_DBAutoCfg.exe /importlicense=<full path to new file>
```

4. Start the MiCollab AM service.

Generate and Import a new Self-Signed SSL Certificate

Each MiCollab AM System Server and Call Server defaults with its own self-signed certificate for use by the system. If needed, a new self-signed certificate can be generated and imported using the following steps:

1. Stop the MiCollab AM service.
2. Run the following command within the container from CX\Bin:

```
AT_DBAutoCfg.exe /sslcertcreate
```

3. Start the MiCollab AM service.

Importing a Custom SSL Certificate

Each MiCollab AM System Server and Call Server defaults with its own self-signed certificate for use by the system. Customers may prefer instead to provide their own custom certificate. Below are the steps to import a custom SSL key/certificate into the container:

1. Stop the MiCollab AM service.
2. Copy the replacement certificate and key PEM files into the container.
3. Run the following command within the container from CX\Bin:

```
AT_DBAutoCfg.exe /sslcertimport /certfile=<full path to certificate PEM file>  
/keyfile=<full path to key PEM file>
```

4. Start the MiCollab AM service.

Resetting an administrator password

If a scenario arises where the password of a Tenant Administrator or Site Administrator needs to be reset to the system default, and another account is unable to perform the action through the MiCollab AM Administration client, it can be done from the command line on the System Server container, providing the name of the administrator account. The following example resets the default Site Administrator account to the default empty password.

```
AT_DBAutoCfg.exe /resetpassword /account=siteadmin
```

Note that for security reasons, because the password is reset to the published default password, the password must be changed upon the next logon using this account.

Resetting the automatic FTPS password

Containerized MiCollab AM uses FTPS for copying files between the System Server and any Call Servers. The FTPS configuration uses a unique password which is auto generated when each server is initialized. However, there may be times when customers want to reset the password, such as for security reasons. To reset the FTPS password to a new, auto-generated password, run the following command within the container from CX\Bin:

```
AT_DBAutoCfg.exe /ftppasswordreset
```

NOTE This can be done while MiCollab AM is running, however there may be a very brief period where files fail to copy on a very active system.

Licensing

To acquire a valid license for containerized MiCollab AM, contact your MiCollab AM account representative. They will provide a license file specific to your deployment. This may involve first running the following utility on the System Server container and copying and sending the output fingerprint codes.

```
C:\EchoID_CLI.exe
```

Appendix

FTPS for File Copying between Servers

FTPS is automatically configured on containerized MiCollab AM servers and used for copying certain files between the System Server and the Call Server(s), such as local store messages, name recordings, greeting recordings, and announcements. Traditionally MiCollab AM has used the SMB protocol for this purpose, however SMB is not supported on Windows containers, so FTPS is used instead.

NOTE Because SMB is not used for copying files between servers, the MiCollab AM File Manager Service does not require the usual administration-level logon rights, and thus can run under the default Local System account.

By default, the configuration is fully automated, including the creation of a self-signed certificate.

NOTE Customers can use their own certificate by registering it in IIS.

WARNING Changes to IIS are not part of the volume and thus are lost upon redeployment or upgrade.

External Volumes for Data Persistence

By default, MiCollab AM containers are created with a container volume which maps key customer data to persistent storage locations that are stored external to the container. By having data persisted in an external volume, if the container is lost or otherwise needs to be redeployed, this data is automatically mapped to the replacement container, seamless to MiCollab AM.