

MiCollab Advanced Messaging Microsoft Skype for Business SIP Trunk

Integration Technical Note

For version 9.1 and above

Notice

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

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

Trademarks

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

© Copyright 2020, Mitel Networks Corporation

All rights reserved

Contents

Preface	5
About This Guide	5
References	6
Documentation	6
Documentation Updates	6
Help	7
Document Conventions	7
Features Supported by This Integration	8
Critical Application Considerations	11
Installation Requirements	14
Microsoft Application Requirements	14
MiCollab AM Requirements	14
Programming the Skype for Business Server	15
Configuring MiCollab AM as Trusted Application	17
Generating Required Commands Using Provided Script	17
Using Skype for Business Trusted Application Configuration Generator	19
Commands for Configuring MiCollab AM as Trusted Application	23
Creating a New Trusted Application Pool	23
Optionally Adding More Call Servers to the Newly Created pool	24
Configuring the Port Where MiCollab AM Listens for Connections	24
Creating an Endpoint for MiCollab AM	25
Enabling the Changes into Your Skype for Business Topology	25
Using Call Server(s) Configuration Data Export	26
Preparing Certificates for TLS Communication	28
Creating Certificate for Trusted Application Pool	28
Creating Certificate Online	28
Creating Certificate Offline	29
Exporting Certificates Needed to Configure MiCollab AM	31
Importing Certificates into the Computer Hosting the MiCollab AM Call Server	33
Configuring Call Forwarding for Skype for Business Clients	35
Configuring MiCollab AM	42
Configuring MiCollab AM for the Integration During Initial Installation	42
Configuring Existing MiCollab AM for the Integration	50

Configuring the Extension Device for Subscribers	59
Configuring a SIP URI Extension Device for Subscribers	61
Configuring MWI for Polycom Phones	62
Configuring MiCollab AM for SIP Failover	63
Configuring Direct-Inward-Dial (DID) Call Routing to MiCollab AM	66
Configuring MiCollab AM to Accept a DID Call Directly on Behalf of a Subscriber	67
Enabling Gateway Support	69
Critical Application Considerations	69
Programming the Skype for Business for Gateway Support	69
Creating Secondary Endpoint	70
Creating and Registering Skype for Business Server Application	70
Creating Normalization Rule to Add the Routing Prefix	73
Configuring MiCollab AM for Gateway	73
Changing the Network Binding Order on the MiCollab AM Platform	74
Windows Server 2012 R2	74
Windows Server 2016 / 2019	75
Configuring Quality of Service (QoS)	76
Appendix A – Converting Trusted Application Pool Certificate from PFX Format to PEM	77
Appendix B – Configuring MiCollab AM to Use Certificate Files Directly	78

Preface

About This Guide

IMPORTANT Any integration procedures and content written for **Skype for Business Server 2015** or **Skype for Business Server 2019** in this document also apply to **Microsoft Lync 2013**.

This Integration Technical Note (ITN) is written for dealers who are experienced with MiCollab Advanced Messaging (MiCollab AM) and who are familiar with its procedures and terminology. It also assumes that you are familiar with the features and functionality of the Microsoft Skype for Business Server 2015 or Skype for Business Server 2019 and are able to create and modify scripts on that server, referred to as "Skype for Business Server" within this document.

This document describes how to integrate MiCollab AM with Skype for Business Server, using the Session Initiation Protocol (SIP) integration, which consists of registering MiCollab AM as a trusted application for Skype for Business Server and configuring MiCollab AM.

MiCollab AM uses SIP trunks to integrate with the Skype for Business Server. This integration operates exclusively over an IP-based network; it uses no analog or digital voice telephony ports, but passes voice communication and signaling information over the network. The Call Server provides the hunting to an available line on the Call Server.

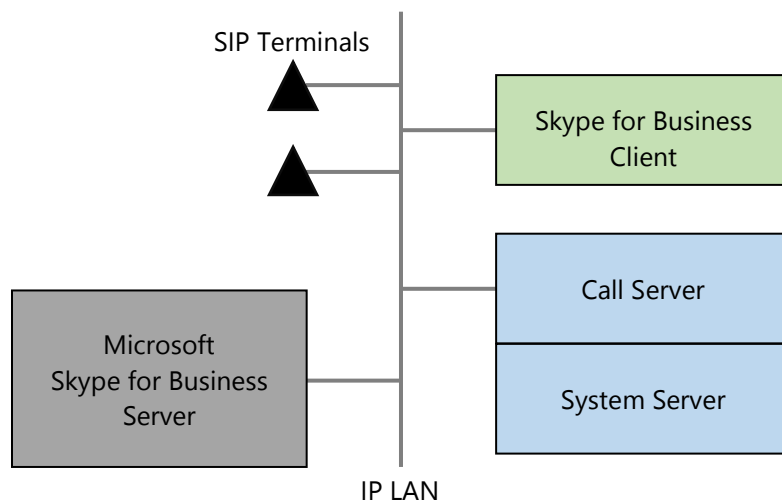


Figure 1. SIP Terminals

This document also describes the critical application considerations with which you should be familiar before you begin work on the integration.

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 detailed documents, refer to the following list of references:

Table 1. References

Document Type	Document Title
Administration Documentation	<i>System Administration Guide</i>
Server Documentation	<i>System Installation and Configuration Guide</i>
Online help	MiCollab AM online help system

For specific information about Skype for Business Server 2015, Skype for Business Server 2019, or Microsoft Lync 2013, see the Microsoft documentation.

Features Supported by This Integration

The following tables list the features supported with the Skype for Business Server integration.

Table 2. Call Forward to Personal Greeting Support for Common Call Types

Divert to MiCollab AM on	Supported	Notes
No Answer	Yes	
Busy	Yes	Note 1
Forward All	Yes	
Do Not Disturb	Yes	Note 1

NOTES

1. Skype for Business cannot be configured for **Call Forward Busy** or **Call Forward Do Not Disturb** but it is possible to work around this by installing the **Skype for Business Routing on Busy** application Skype for Business Front End server.
For more information, refer to the [Configuring Call Forwarding for Skype for Business Clients](#) section.
2. If Skype for Business basic client is used, then the user will not be able to configure call forwarding.
In this scenario, you need to use the **Secondary Extension Feature Activation Utility** (SEFAUtil) application to configure call forwarding settings.
For more information, refer to the [Configuring Call Forwarding for Skype for Business Clients](#) section.

Table 3. Integration Features Supported for Microsoft Skype for Business Server

Feature	Supported	Notes
Automatic subscriber logon	Yes	
ANI/CLI	Yes	

Announce Busy greeting on forward busy calls	Yes	Note 1
Call screening	Yes	
Caller queuing	No	
DNIS	Yes	
End-to-end DTMF, attendant console	Yes	
End-to-end DTMF, proprietary telephones	Yes	
Fax Detection	Yes	
Internal calling party ID for reply	Yes	
Live record, integrated	No	
Live reply to sender	Yes	
Message notification callouts	Yes	
MWI, set/clear	Yes	Note 2
MWI, inband/outband	Inband	
Networking, analog	No	
Overflow from MiCollab AM to attendant	N/A	
Overflow to MiCollab AM from attendant	N/A	
PBX-provided disconnect signaling	N/A	
S RTP	Yes	
TLS	Yes	
Transfers, blind	Yes	
Transfers, confirmed	Yes	
Transfers, supervised	Yes	
Transfers, monitored	Yes	
Trunk ID for call routing	No	
Multiple integrations	Yes	Note 3

NOTES

1. This feature is supported only if the **Skype for Business Routing on Busy** application is installed on Skype for Business Front End server.
For more information, refer to the [Configuring Call Forwarding for Skype for Business Clients](#) section.
2. MWI is supported on Polycom CX500 and CX600 phones only.
For more information, refer to the [Configuring MWI for Polycom Phones](#) section.
3. See [Critical Application Considerations](#).

Critical Application Considerations

Known limitations or conditions within the Skype for Business Server and MiCollab AM that affect the performance are listed here. General recommendations are provided when ways to avoid these limitations exist.

- 911 and E.911 are not supported via the integration.
- Skype for Business cannot be configured for **Call Forward Busy**. As an option Skype for Business allows the user to receive a notification of an incoming call during an active call and redirect the incoming call to a destination of the user's choice. However, it is possible to work around this by installing the **Skype for Business Routing on Busy** application on Skype for Business Front End server.

For more information, refer to [Configuring Call Forwarding for Skype for Business Clients](#).

- Skype for Business cannot be configured for **Call Forward Do Not Disturb (DND)**. **DND** will always override any call forwarding settings you have setup and caller will receive busy tone if call is placed to a user in **DND** mode. However, it is possible to work around this by installing the **Skype for Business Routing on Busy** application on Skype for Business Front End server.

For more information, refer to [Configuring Call Forwarding for Skype for Business Clients](#).

- **Message Waiting Indicator (MWI)** is supported on Polycom CX500 and CX600 phones only with the Skype for Business integration.
- Skype for Business Mac client version 16.18.51 or prior versions do not support integrated call because no Tel URI is provided. In this case, you should configure a SIP URI extension device in addition to an extension device for support of integrated call. For more information, refer to the procedure in [Configuring a SIP URI Extension Device for Subscribers](#).
- Each Skype for Business user that is supported by MiCollab AM must have a Subscriber mailbox on MiCollab AM.

In addition, each subscriber must have an extension device assigned to the integration's switch section. This number should be the same as the number assigned to the **Line URI** in Skype for Business for the user without the '+' sign.

- Skype for Business Server prefers telephone numbers in **E.164** format. In order for MiCollab AM to be able to dial numbers, you need to create a dial plan with normalization rules and configure MiCollab AM to use it.

IMPORTANT Please be aware that MiCollab AM does not add the '+' sign when dialing numbers.

- Subscribers must have the appropriate callout permission on MiCollab AM to enable them to place calls to numbers that are not associated with other subscribers via their devices configuration.
- It must be the first network connection in the network binding order. If your MiCollab AM server platform is a component of two or more local or wide area networks (LANs or WANs), you must make sure that this integration does not interfere with the normal network operation of the server.

For more information, refer to [Changing the Network Binding Order on the MiCollab AM Platform](#).

- MiCollab AM 9.1 supports up to 10 integration types (i.e., licensed integrations) in total per system. However, the following limitations apply to each Call Server:
 - Limited to 3 integration types per Call Server
 - The 3 integration types can be any mix of TDM and SIP (e.g., 1 TDM and 2 SIP)
 - Limited to 1 Cisco UCM SCCP IP integration. Can be mixed with TDM, but not with SIP
 - Connect up to 10 telephone systems total per Call Server (e.g., 2 Genband SIP Trunk systems using SIP + 5 Avaya IP Office systems using SIP + 3 Siemens HiPath 4000 systems using Station Set Emulation)
 - SIP timers for Aastra EETS integrations are incompatible with other SIP integrations. Thus, it is not possible to have an EETS integration with any other SIP integration on the Call Server.
- The MiCollab AM **Integration Options** parameter, **Validate Remote Hosts for Media** validates each incoming audio packet and accepts it only if it is sent from a valid endpoint. The parameter is disabled by default. Enabling this parameter causes MiCollab AM to reject RTP packets from invalid endpoints, rejects MWI packets that timeout after a specified number of times, and overcomes port lockups when callers hang up while MiCollab AM is performing a blind transfer.

IMPORTANT Enabling this parameter causes processing overhead and should only be enabled when necessary.

- It is recommended to use Windows Server 2016 or later for Integrations that use Session Initiation Protocol (SIP) Transport Layer Security (TLS) when FIPS is enabled on MiCollab AM. Older versions of Windows use algorithms that are not FIPS compliant to export the certificate information used for TLS. Because of this, MiCollab AM will not be able to access certificate-related data.

Installation Requirements

Review the following information before performing any of the procedures in this document. To install this successfully, you must meet the installation requirements for both the Skype for Business Server and MiCollab AM.

Microsoft Application Requirements

- Microsoft Lync 2013 version 5.0.8308.556 or later (cumulative patch October 2013)
- Microsoft Skype for Business Server 2015 version 6.0.9319.102 (Cumulative patch November 2015) or prior supported versions
- Microsoft Skype for Business Server 2019 version 7.0.2046.0 or later

You can find more information about the Skype for Business Server on the Microsoft website:
products.office.com/en-us/skype-for-business/

MiCollab AM Requirements

- MiCollab AM software version 6.0 SU1 or later (with Microsoft Lync 2013)
- MiCollab AM software version 6.1 SU2 or later (with Microsoft Skype for Business Server 2015)
- MiCollab AM software version 9.0 SU2 or later (with Microsoft Skype for Business Server 2019)
- At least one 100 MB or 1000 MB network interface card and cable
- MiCollab AM software key diskette or feature file with the Microsoft Skype for Business Server SIP integration enabled and one Virtual SIP, RTP and ICE license enabled for each port

Programming the Skype for Business Server

Follow the recommendations and programming examples in this section to configure MiCollab AM as a trusted application for the Skype for Business Server. Programming examples show commands and parameters that are necessary for integration. They do not represent programming in its entirety.

The installing technician should be familiar with programming the Microsoft Skype for Business Server and with the necessary steps to configure trusted applications for Skype for Business Server.

See the Microsoft Skype for Business Server documentation or the online help for specific information on programming the Skype for Business Server.

The steps you must take to configure MiCollab AM as a trusted application for Skype for Business Server are as follows:

- Create a trusted application pool and add the computer that will host MiCollab AM system server to this pool and all the computers that will host MiCollab AM call servers.
- Create a trusted application to register MiCollab AM listening port.
- Create a trusted application endpoint to associate a SIP address and LineURI with MiCollab AM.

NOTE MiCollab AM requires the user field of the SIP address to be the number specified in LineURI without the '+' sign.

- Prepare the certificates needed to configure MiCollab AM for TLS.

NOTE Skype for Business Server prefers telephone numbers in E.164 format. In order for MiCollab AM to be able to dial numbers, you need to create a dial plan with normalization rules and configure MiCollab AM to use it.

When creating the normalization rule, be aware that MiCollab AM does not add the '+' sign when dialing numbers.

The sample configuration in this programming section uses the following components:

Table 4. Sample Configuration for Microsoft Skype for Business Server

Component	Description
sfbdomain.local	Domain hosting Skype for Business Server deployment
SFB.sfbdomain.local	FQDN for the Skype for Business Front End pool
SFB-FE1.sfbdomain.local	FQDN for the Front End server in the SFB.sfbdomain.local pool

CS1.sfbdomain.local	FQDN for the computer that will host MiCollab AM call server
CS2.sfbdomain.local	FQDN for the computer that will host another MiCollab AM call server
cx-trusted-apps.sfbdomain.local	FQDN for the trusted application pool
cx-voicemail	Trusted application ID for MiCollab AM
5061	TLS listening port for MiCollab AM
1600	Phone number associated with MiCollab AM (pilot number users dial)

Configuring MiCollab AM as Trusted Application

Follow the procedures in this section to register MiCollab AM as a trusted application for Skype for Business Server. This section is a list of **cmdlets** that you need to execute in Skype for Business Server Management Shell.

Generating Required Commands Using Provided Script

Several PowerShell commands must be executed in order to configure MiCollab AM as a trusted application for Skype for Business, and each of these commands has a relatively long list of arguments that need to be specified.

To simplify this process, MiCollab AM provides a configuration PowerShell script that can be used to generate the arguments for these commands based on your input provided through a configuration form. In addition, the script can be used to export the necessary configuration data for MiCollab AM call server(s).

This **Skype for Business integration configurator** script can be found under the MiCollab AM installation folder: **\Server Installs\Telephony Server\Server\Tools\Scripts\Lync\CX-Lync-Integration-Configurator.ps1**

It is recommended to run the script with elevated privileges using the **Skype for Business Management Shell**.

In addition, the generated Skype for Business commands that configure the new trusted application should be executed on the same computer. This is required in order for the script to export the certificate for the trusted application – if this certificate is generated using the **Request-CsCertificate** command – and the root in the certificates chain of the Skype for Business server certificate.

NOTE The script uses the read-only PowerShell **cmdlets** and as such it can be run under a read-only Skype for Business administrator account – an account that is a member of **CSVViewOnlyAdministrator**.

The script can be executed remotely on a computer without Skype for Business Management Shell.

However, in this case, the script will not be able to export the certificate for the trusted application or the root in the certificates chain of the Skype for Business server certificate – these will have to be configured manually.

The manual process of configuring these certificates for MiCollab AM is presented in a later section of this document.

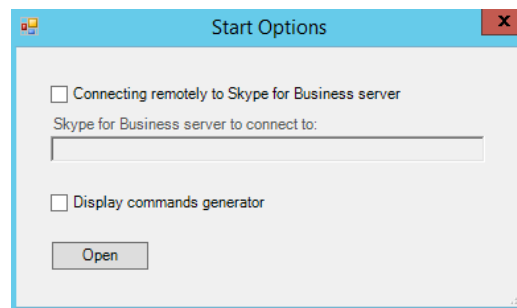
If the certificate for the trusted application is provided through an alternative method – not using **Request-CsCertificate** – there is no need to run the script with elevated privileges. Also, in this scenario, there is no need to run the script on a computer with the Skype for Business Management Shell – it can be executed remotely.

To execute the script:

- 1 Type the script path in PowerShell or the **Skype for Business Management Shell** instance.

NOTE If the shell is configured not to run any script and you do not want to enable the ability to run scripts, then you can simply copy and paste the content of the file into the shell. The script is signed and the shell should be able to run it if the execution policy is set to **AllSigned** or **RemoteSigned**.

- 2 The script first displays a form enabling you to specify if the current instance is being executed on a computer with the Skype for Business Management Shell installed or on a remote computer.



When executing it remotely, you must select the **Connecting remotely to Skype for Business server** option and specify the front end server that the script should use to retrieve the Skype for Business related data.

NOTE When the script is executed remotely, there will be a relatively long delay after the **Open** button is clicked. This delay is generated by the fact that the script must download details about the **cmdlets** that can be executed in the remote session.

- 3 Decide if the script will display the full configuration form or only the export form.
 - If a new trusted application must be created, then the **Display commands generator** option should be checked. This way, the script will display the **Skype for Business trusted application configuration generator** form that enables you to select or input values that will be used to construct the commands necessary to create the new trusted application.
 - The script will populate many of the fields with data from the target Skype for Business deployment. In addition, it will provide default values for most of the other parameters. In many cases you will only have to specify the FQDN of the computer(s) that will host MiCollab AM call server(s) and accept all other default values.
- 4 Once all parameters have a value, the script will use these values to generate and display a list with all commands, including their parameters, which have to be executed in order to create the new trusted application.
- 5 After an administrator with the *write* rights executes these commands successfully, click the **Generate call server(s) info** button to generate the configuration information for the MiCollab AM

call server(s). More details are provided in the [Using Skype for Business Trusted Application Configuration Generator](#) section.

- 6 If the trusted application already exists in the Skype for Business deployment, leave the **Display commands generator** option unchecked.

This way, the script will display a simple export form where you will select a trusted application and a dial plan. Using the properties of the selected trusted application, the script will generate the configuration information for the MiCollab AM call server(s).

More details are provided in section [Using Call Server\(s\) Configuration Data Export](#) section.

Using Skype for Business Trusted Application Configuration Generator

This form is used to select or input values for the parameters of the commands that have to be executed in order to create a new trusted application for MiCollab AM. In addition, the form allows you to generate the configuration data for MiCollab AM call server(s), after the trusted application is configured in Skype for Business.

Skype for Business trusted application configuration generator

Registrar:
SFB2015.sfbdomain.local
SFB2015.sfbdomain.local

Site:
Main
Main

Sip domain:
sfbdomain.local
sfbdomain.local

Dial plan [simple names]:
DefaultProfile
DefaultProfile

Certification authority:
MASTERCA.sfbdomain.local\SFBDOMAIN-CA
MASTERCA.sfbdomain.local\SFBDOMAIN-CA

Trusted application pool FQDN:
cx-trusted-apps.sfbdomain.local

Trusted application name:
cx-voicemail

Trusted application port:
5061

E.164 number [without '+']:
1600

Trusted application display name:
Voicemail

Sip address:
sip:1600@sfbdomain.local

Line URI:
TEL:+1600

Call server(s) FQDN:
Add .sfbdomain.local
CS1.sfbdomain.local
CS2.sfbdomain.local
Remove

Commands to create trusted application:
1. Command for creating a new trusted pool for the computers that will host the trusted application
New-CsTrustedApplicationPool -Identity 'cx-trusted-apps.sfbdomain.local' -Registrar 'SFB2015.sfbdomain.local' -ComputerFqdn 'CS1.sfbdomain.local' -Site

Figure 2. Skype for Business Trusted Application Configuration Generator

- Registrar:** The script will populate this list with the FQDNs of all pools configured in the Skype for Business deployment that provide the Registrar service.
 You should select the FQDN of the pool that should manage the end point for the new trusted application.
- Site:** The script will populate this list with the IDs of all sites configured in the Skype for Business deployment.
 You should select the ID of the site in which the pool for the new trusted application is homed.
- Sip domain:** The script will populate this list with the identities of all SIP domains configured in the Skype for Business deployment, authorized for SIP traffic.
 You should select the SIP domain that will be used to construct the sip address of the end point associated with the new trusted application.

- **Dial plan [simple name]:** The script will populate this list with the simple name of all dial plans defined in the Skype for Business deployment.

You should select the dial plan that should be used by the MiCollab AM call server(s) when making callouts.

NOTE This information is not used when constructing the commands necessary to configure the new trusted application, but will be used when generating the configuration data for MiCollab AM call server(s).

- **Certification authority:** The script will populate this list with the identities of all certification authorities configured in the Active Directory.

You should select the certification authority that will be used to generate certificates for the new trusted application.

NOTE Skype for Business PowerShell cmdlet **Request-CsCertificate** can be used to generate the appropriate certificate for the new trusted application. This is the recommended approach since the certificate will be used strictly for communication of MiCollab AM call server(s) with Skype for Business servers and because this method of generating the certificate is faster, easier and less prone to errors.

If **Request-CsCertificate** will be used to generate the certificate, then you must select one of the certification authorities in this list. If **Request-CsCertificate** will not be used, then this field can be ignored.

- **Trusted application pool FQDN:** You should enter in this field the FQDN of the new trusted application pool.

NOTE The script will populate this field with a string obtained by concatenating 'cx-trusted-apps' name with the domain of the currently selected registrar.

- **Trusted application name:** You should enter in this field a unique name to identify the new trusted application.

NOTE This name is not displayed to users and it used internally by Skype for Business. The script will populate this field with 'cx-voicemail'

- **Trusted application port:** You should enter in this field a network port that MiCollab AM call server(s) will use to listen for connections from Skype for Business.

NOTE The default value used by MiCollab AM for secured SIP communication is: 5061. The script will populate this field with 5061.

- **E.164 number:** You should enter in this field a unique number to be associated with the end point for the new trusted application.

NOTE The number must not contain the '+' prefix.

The script uses this number to generate the sip address and the line URI properties for the end point associated with the new trusted application. The generated sip address and line URI are displayed in read-only text boxes under this field.

MiCollab AM requires the user name part of the sip address to match the number from line URI.

- **Trusted application display name:** You should enter in this field the string that will be displayed on the Skype for Business clients when in conversation with MiCollab AM.
- **MiCollab AM call server(s) FQDN:** You should enter in this list all the MiCollab AM call servers that will be communicating with Skype for Business.

NOTE The FQDN should be provided. If for any reason the IP is being used or the MiCollab AM call server(s) are not part of the domain hosting the Skype for Business deployment, the **New-CsTrustedApplicationComputer** command will generate a warning about the computer missing from Active Directory. This warning can be ignored.

For convenience, the script will populate the field with the domain name. You only have to add the computer name in order to obtain the FQDN.

After entering the FQDN of a call server, click the **Add** button to add it to the list. The script will use only the items in the list.

To remove an entry from the list click the **Remove** button.

- **Commands to create trusted application:** The script will use this text box to display generated commands. Each command is prefixed by a short comment about the command and this comment includes the order in which the commands have to be run. The order to execute them also matches the display order.

NOTE Detailed information about each of the generated commands will be provided later in this document.

A Skype for Business administrator will have to execute these commands in order to create the new trusted application, its pool and its end point. The commands must be executed in the specified order.

The **Copy** button will copy the entire content of this text box – all commands – to clipboard.

The **Save** button allows you to save the content of this text box to a file.

The commands used in this field are explained in details in the following [Commands for Configuring MiCollab AM as Trusted Application](#) section.

- **Generate call server(s) info:** This button can be used to generate a configuration file for MiCollab AM call server(s), after a Skype for Business administrator executes the generated commands and configures the new trusted application.

Once this button is clicked, the script will start collecting required information about the newly configured trusted application and prepare the content of the configuration file for MiCollab AM call server(s).

If the script is able to retrieve a suitable certificate for the trusted application, then it will prompt you to provide a password to encrypt the certificate when exporting it to the configuration file. This password will be required when importing the configuration data into MiCollab AM.

NOTE The following are required in order for the script to be able to locate a suitable certificate: a certificate that has the trusted application pool name as subject, must be present in the

Windows certificate store for the local computer. The subject alternative name of the certificate must contain the FQDNs of all MiCollab AM call server(s) configured in the trusted application.

The script should have been started with elevated privileges in order for it to be able to access the Windows certificate store for the local computer.

When executed, the generated **Request-CsCertificate** command will send a properly formed request to the indicated certification authority which will be able to generate a suitable certificate. In addition, the **Request-CsCertificate** command will also retrieve the generated certificate and import it in the Windows certificate store for the local computer.

This is the reason why the script should be started under elevated privileged on the computer where the generated commands will be executed to configure the new trusted application. The script can run under the account of a Skype for Business read-only administrator – a member of **CSViewOnlyAdministrator** group.

After preparing the configuration data for the MiCollab AM call server(s), the script will prompt you to specify the path of the file to save this data.

The saved file should be copied to a location accessible to the MiCollab AM call server(s). Using the MiCollab AM system configuration tool, the data can be imported into MiCollab AM.

NOTE The same file will contain configuration data for all MiCollab AM call servers specified in the **Call server(s) FQDN** list.

Commands for Configuring MiCollab AM as Trusted Application

NOTE These commands can be used through the Skype for Business Trusted Application Configuration Generator or as standalone through PowerShell.

Creating a New Trusted Application Pool

The **New-CsTrustedApplicationPool** cmdlet is used to create a new trusted application pool that will contain the computer(s) hosting MiCollab AM call server(s).

```
New-CsTrustedApplicationPool -Identity 'cx-trusted-apps.sfbdomain.local' -Registrar 'SFB.sfbdomain.local' -ComputerFqdn 'CS1.sfbdomain.local' -Site 'Main' -RequiresReplication $false
```

Table 5. Required Arguments for New-CsTrustedApplicationPool Command

Argument	Description
Identity	Unique FQDN for the new trusted application pool
Registrar	The service ID or FQDN of the Registrar service for the pool

NOTE You can run **Get-CsService -Registrar** to obtain the FQDN of the registrar.

Site The Site ID of the site in which this pool is homed

NOTE You can run **Get-CsService -Registrar** to obtain this ID

ComputerFqdn FQDN for the MiCollab AM system server

RequiresReplication Set this to *\$false*. MiCollab AM is a manually-provisioned application.

NOTE For more information about this command, see: technet.microsoft.com/en-us/library/gg425804.aspx.

Optionally Adding More Call Servers to the Newly Created pool

```
New-CsTrustedApplicationComputer -Pool cx-trusted-apps.sfbdomain.local -Identity "CX-CS.sfbdomain.local"
```

Table 6. MiCollab AM Configuration - Call Servers (Optional)

Argument	Description
Pool	FQDN of the new pool – specified in New-CsTrustedApplicationPool
Identity	FQDN of the new MiCollab AM call server to add

NOTE For more Description information about this command, see: technet.microsoft.com/en-us/library/gg398405.aspx.

Configuring the Port Where MiCollab AM Listens for Connections

NOTE Remember this port number, as you will need it later when configuring MiCollab AM. By default, MiCollab AM uses 5061 for TLS/MTLS enabled connections.

```
New-CsTrustedApplication -TrustedApplicationPoolFqdn cx-trusted-apps.sfbdomain.local -ApplicationId cx-voicemail -Port 5061
```

Table 7. Port Configuration

Argument	Description
TrustedApplicationPoolFqdn	FQDN of the new pool – specified in New-CsTrustedApplicationPool

ApplicationId	The name of the application. This must be a string that is unique within the pool that is specified in the TrustedApplicationPoolFqdn parameter
Port	Port number to be used by MiCollab AM to connect to Skype for Business Server

NOTE For more information about this command, see: technet.microsoft.com/en-us/library/gg398259.aspx.

Creating an Endpoint for MiCollab AM

This command creates the SIP address and telephone number that will be assigned to MiCollab AM.

NOTE Remember the phone number, as you will need to set it as the *Hunt Group Access Code* when configuring MiCollab AM.

```
New-CsTrustedApplicationEndpoint -TrustedApplicationPoolFqdn cx-trusted-apps.sfbdomain.local -ApplicationId cx-voicemail -SipAddress sip:1600@sfbdomain.local -LineURI "tel:+1600" -DisplayName "MiCollab AM Voicemail"
```

Table 8. Endpoint Configuration

Argument	Description
TrustedApplicationPoolFqdn	FQDN of the pool – specified in New-CsTrustedApplicationPool
ApplicationId	The name of the application as specified in the command New-CsTrustedApplication
SipAddress	SIP address that will be associated with MiCollab AM
	NOTE The user field of the SIP address must be the LineURI number assigned to MiCollab AM. Do not include the '+' sign.
LineURI	Number assigned to MiCollab AM preceded by "tel:+" prefix
DisplayName	Display name to be used by Skype for Business clients when referencing to this SIP address

NOTE For more information about this command, see: technet.microsoft.com/en-us/library/gg398594.aspx.

Enabling the Changes into Your Skype for Business Topology

The **Enable-CsTopology** cmdlet must be used in order to enable the changes made through the **cmdlets** presented above in Skype for Business.

Enable-CsTopology

NOTE For more information about this command, see: technet.microsoft.com/en-us/library/gg398398.aspx.

Using Call Server(s) Configuration Data Export

The configuration script provided with MiCollab AM can be used to export the configuration data for the MiCollab AM call server(s) configured as trusted computer(s).

Details about the location and execution of this script can be found in previous [Generating Required Commands Using Provided Script](#) section.

When the **Display commands generator** option is unchecked, the script will display a simple form that allows the export of the configuration data based on previously configured trusted application.

Call server(s) config data export

Dial plan [simple names]:

DefaultProfile

Trusted application:

cx-trusted-apps.sfbdomain.local/um:application:cx-voicemail
sfbpool.sfbdomain.local/um:application:sefautil

Application endpoint:

sip:1600@sfbdomain.local

Generate call server(s) info

Figure 3. Call Server Configuration Data Export

This form allows you to select an existing trusted application and generate the configuration for MiCollab AM call server(s). The configuration data will allow MiCollab AM call server(s) to connect to Skype for Business and communicate with Skype for Business clients.

- **Dial plan [simple name]:** The script will populate this list with the simple name of all dial plans defined in the Skype for Business deployment.

You should select the dial plan that should be used by the MiCollab AM call server(s) when making callouts.

- **Trusted application:** The script will populate this list with the identities of all trusted applications configured in the Skype for Business deployment.

You should select the identity of the trusted application configured for the current MiCollab AM deployment.

- **Application end point:** The script will populate this list with the sip address of all end points configured for the selected trusted application.

You should select the sip address of the end point that will be used by the current MiCollab AM deployment.

- **Generate call server(s) info:** This button will be used to generate the configuration file for MiCollab AM call server(s).

Once this button is clicked, the script will start collecting required information about the selected trusted application and prepare the content of the configuration file for MiCollab AM call server(s).

If the script is able to retrieve a suitable certificate for the trusted application, then it will prompt you to provide a password to encrypt the certificate when exporting it to the configuration file. This password will be required when importing the configuration data into MiCollab AM.

NOTE The following are required in order for the script to be able to locate a suitable certificate: a certificate that has the trusted application pool name as subject, must be present in the Windows certificate store for the local computer. The subject alternative name of the certificate must contain all of the MiCollab AM call server FQDNs.

The script should have been started with elevated privileges in order for it to be able to access the Windows certificate store for the local computer.

If the **Request-CsCertificate** command was used to generate the appropriate certificate, then the script should be started under elevated privileged on the computer where the **Request-CsCertificate** command was executed.

This is required because the **Request-CsCertificate** command imports the newly generated certificate in Windows certificate store for the local computer where it is executing. The script can run under the account of a Skype for Business read-only administrator – a member of **CSViewOnlyAdministrator** group.

After preparing the configuration data for the MiCollab AM call server(s), the script will prompt you to specify the path to save this configuration file.

The saved file should be copied to a location accessible to MiCollab AM call server(s). Using the MiCollab AM system configuration tool, the data can be imported into MiCollab AM.

NOTE The same file will contain configuration data for all trusted computers, part of the trusted application pool hosting the selected trusted application.

All MiCollab AM call servers should be trusted computers in this pool.

Preparing Certificates for TLS Communication

Follow the procedures in this section to prepare the certificates that need to be configured in MiCollab AM to enable TLS communication with Skype for Business Server.

Creating Certificate for Trusted Application Pool

A certificate that is intended to be configured on MiCollab AM in order to enable SIP communication with the Skype for Business server, must meet the following requirements:

- The Subject Name (SN) of the certificate should be set to the trusted application pool FQDN.
- The Subject Alternative Name (SAN) of the certificate should list the trusted application pool FQDN and the trusted application computer FQDN.

NOTE Same certificate can be used for multiple MiCollab AM call servers. The Subject Alternative Name (SAN) of such certificate must list the FQDNs of all computers where it will be used.

Skype for Business provides the **Request-CsCertificate** cmdlet that can be used to make both online and offline requests for new certificates. This command simplifies the process of generating new certificates by creating a request that contains proper values for the subject name and subject alternative name fields based on the topology of the Skype for Business deployment.

Creating Certificate Online

This is the recommended approach as it is the easiest and less error prone method.

NOTE This certificate will be used only for the SIP communication between MiCollab AM and Skype for Business Front End servers. MiCollab AM does not communicate directly with Skype for Business clients. This communication will be relayed through front end servers.

As such, the certificate needs to be trusted only by the front end servers.

If the **CA** argument specifies the identifier of a certification authority from the domain, then the **Request-CsCertificate** cmdlet will automatically execute all of the following actions:

- Generate proper certificate signing request based on the provided information and data retrieved from topology
- Send the request to the specified certification authority
- Download the signed certificate and import it into the personal Windows certificate store for local machine where the command is being executed

Use the following PowerShell command to request a certificate for the trusted application pool:

```
Request-CsCertificate -New -Type Default -CA 'MASTERCA.sfbdomain.local\SFBDOMAIN-CA'
-FriendlyName 'cx-trusted-apps.sfbdomain.local Pool' -ComputerFqdn
'CS1.sfbdomain.local' -DomainName 'CS1.sfbdomain.local, CS2.sfbdomain.local' -
PrivateKeyExportable $true
```

Table 9. Required Arguments for Request-CsCertificate command [online]

Argument	Description
New	A new certificate will be requested.
Type	Should be set to Default .
CA	Fully qualified domain name (FQDN) that points to the CA (Certification Authority) NOTE To obtain a list of known CAs, type Certutil at the Windows PowerShell prompt, and then press ENTER . The Config property returned by Certutil indicates the location of a CA.
FriendlyName	User-assigned name that makes it easier to identify the certificate.
ComputerFqdn	FQDN for MiCollab AM system server.
DomainName	FQDN for all computers in the trusted application pool, separated by commas.
PrivateKeyExportable	This argument must be set to \$true . MiCollab AM requires both the certificate and its private key.

NOTE For more information about this command, see: technet.microsoft.com/en-us/library/gg425723.aspx.

NOTE If the selected certification authority is not configured to automatically issue the certificates, then the execution of the **Request-CsCertificate** cmdlet will terminate with a status indicating that the request is pending.

In this case, an administrator should manually issue the certificate from the certification authority system. Once the certificate is issued, the **Request-CsCertificate** command must be executed again but using only the **-Retrieve** argument: **Request-CsCertificate -Retrieve**

Creating Certificate Offline

If for any reason, the online method presented above cannot be used, then the following steps can be executed in order to create a new certificate for the trusted application:

- Run the **Request-CsCertificate** cmdlet so that it will generate the proper certificate signing request and save it to a file instead of automatically sending it to a certification authority. This can be obtained by executing the command without **CA** argument but with the **Output** argument, as in the next example.

- Send the certificate signing request to a certification authority in order to retrieve the signed certificate
- Use the **certreq.exe** Windows utility to import the signed certificate on the same computer that generate the request.

Use the following PowerShell command to generate a certificate signing request for the trusted application pool:

```
Request-CsCertificate -New -Type Default -FriendlyName 'cx-trusted-
apps.sfbdomain.local Pool' -ComputerFqdn 'CS1.sfbdomain.local' -DomainName
'CS1.sfbdomain.local, CS2.sfbdomain.local' -PrivateKeyExportable $true -Output
'C:\Temp\call-servers-certificate.csr'
```

Table 10. Required Arguments for Request-CsCertificate command [offline]

Argument	Description
New	A new certificate will be requested.
Type	Should be set to Default .
FriendlyName	User-assigned name that makes it easier to identify the certificate.
ComputerFqdn	FQDN for MiCollab AM system server.
DomainName	FQDN for all computers in the trusted application pool, separated by commas.
PrivateKeyExportable	This argument must be set to \$true . MiCollab AM requires both the certificate and its private key.
Output	The path of the file where the cmdlet will save the certificate signing request. This file must be sent to the certification request in order to receive the signed certificate to be use by MiCollab AM.

NOTE For more information about this command, see: technet.microsoft.com/en-us/library/gg425723.aspx.

Use the following PowerShell command to import the signed certificate on the machine where the certificate request was created:

```
.\certreq.exe -accept 'C:\Temp\call-servers-certificate.cer'
```

NOTE This example assumes that the signed certificate retrieved from the certification authority was saved on the computer that generated the request in the file: **C:\Temp\call-servers-certificate.cer**.

The certificate must be imported on the computer where the certificate signing request was generated because the private key associated with the certificate is saved on that computer. The **Request-CsCertificate** cmdlet generates both the private key and the certificate signing request.

Once the certificate is imported successfully, it can be exported along with its private key and imported to the call server(s) to be used by MiCollab AM

Exporting Certificates Needed to Configure MiCollab AM

In order for MiCollab AM to communicate with Skype for Business as a trusted application, a certificate that is trusted by the Skype for Business is required.

If the required certificate for MiCollab AM was generated using one of the methods from the previous sections, then the certificate and its private key must be exported from the computer where it was created using the steps described next. During MiCollab AM configuration, the exported certificate will be imported on the computer hosting MiCollab AM.

NOTE This procedure should not be performed if the certificate was generated using a different method and it is available along with its key in a format that allows its transport to the MiCollab AM call server(s). It most probably will not work in this scenario.

This step is not necessary if the certificate was created on the computer hosting the MiCollab AM call server.

If the configuration script provided with MiCollab AM is being used to export the configuration data on the same computer where the certificate was created with **Request-CsCertificate** cmdlet, then the script will automatically export the certificate and its key and store it in the generated configuration file. Therefore, this step is not necessary.

However, the script must be executed with elevated privileges in order to be able to access the Windows certificate store for local machine where the certificate is stored.

To export the certificate for the MiCollab AM trusted application:

- 7 In PowerShell, type *mmc* and press **ENTER** to open Microsoft Management Console application on the computer where the **Request-CsCertificate** cmdlet was executed.
- 8 From the **File** menu, select **Add/Remove Snap-in** to add the Certificates snap-in for local computer account.
- 9 To locate the certificate generated using the **Request-CsCertificate** cmdlet, expand and select the **Personal\Certificates** folder. In the list of certificates from this folder locate the certificate using the Issued To and Friendly Name columns.
- 10 The label in the **Issued To** column should be the FQDN of the trusted pool, and the label in the **Friendly Name** column must match the value provided for the **FriendlyName** parameter to the **Request-CsCertificate** command.
- 11 To export the selected certificate, right-click on the certificate and choose **Export** from the **All Tasks** menu.

NOTE In the **Windows certificate export** wizard, the option that exports the private key must be selected.

- 12 Make available to the MiCollab AM call server(s) the file generated by the export wizard.

To export the certificate for the root CA in the certification path of the Skype for Business certificate:

- 1 In order for MiCollab AM to trust the communication with the Skype for Business, MiCollab AM needs to have access to the certificate for the root CA in the certificate path of the Skype for Business certificate.

NOTE In many cases the computer hosting the MiCollab AM will already have this certificate and therefore this step is not necessary except for confirming that the certificate is present.

If the configuration script provided with MiCollab AM is being used to export the configuration data, then the script will automatically export the appropriate certificate and store it in the generated configuration file. Therefore, this step is not necessary.

However, the script must be executed with elevated privileges in order to be able to access the Windows certificate store for local machine where the certificate is stored.

- 2 In PowerShell, type *mmc* and press **ENTER** key to open Microsoft Management Console application on one of the Skype for Business Front End servers.
- 3 From the **File** menu, select **Add/Remove Snap-in** to add the Certificates snap-in for local computer account.
- 4 Locate the certificate used by Skype for Business among the certificates in the **Personal\Certificates** folder.

NOTE To determine the certificate used by Skype for Business you can use the following PowerShell command: **Get-CsCertificate | ? {\$_.Use -eq 'Default'}**

This command will display several properties of the default certificate used by Skype for Business. The value of CN portion of the Subject property will match the label of the certificate in the **Issued To** column in the Certificates snap-in.

- 5 Double-click the certificate to display the content.
- 6 In the **Certificate** dialog, select the **Certification Path** tab.
- 7 On this tab, select the top most node in the Certification path chain and click **View Certificate** to display the information about the root certificate.
- 8 In the new **Certificate** dialog for the root certificate, select the **Details** tab.
- 9 On this tab click **Copy to File** to export the certificate to a file.

NOTE In order to check if this certificate already exists on the computer hosting the MiCollab AM call server(s), follow these steps:

- a Select the **Serial Number** property to display its value.
- b Open the Certificates snap-in for local computer account on the computer hosting the MiCollab AM call server(s).
- c Right-click on the root Certificates (Local Computer) node.
- d From the menu, select the **Find Certificates** option.

- e** In the **Find Certificates** dialog, set the **Look in Field** option to **Serial Number**.
- f** In the **Contains** field, copy the value of the **Serial Number** property for the root certificate. If the certificate is already present, there is no need to export it.
- g** If the certificate is stored in a different location than **Trusted Root Certification Authorities**, it must be copied in this location using the Certificates snap-in copy and paste functionality.

- 10** Make available to the MiCollab AM call server(s) the file generated by the export wizard.

Importing Certificates into the Computer Hosting the MiCollab AM Call Server

In order for MiCollab AM to be able to access the certificates exported through the procedure described earlier in the previous section, these certificates must be imported on the computer(s) hosting the MiCollab AM call servers.

To import certificate for the trusted application:

- 1** Using Windows explorer, on each of the trusted computers that will be hosting MiCollab AM call server(s), select the file containing the export of the certificate and private key for the trusted application.
- 2** Right-click on the certificate and select the option **Install PFX** from the contextual menu.
- 3** In the opening page of the Windows certificate import wizard, select the **Local Machine** store location.
- 4** After confirming the file, in the **Private key protection** page, enter the password used to export the certificate.
- 5** In addition, make sure that the option **Mark key as exportable** is checked.
- 6** In the **Certificate Store** page, select the **Place all certificates in the following store and using the Browse** button.
- 7** Choose the **Personal** store.
- 8** After confirming the selections, on the last page, click the **Finish** button to complete the import operation.

To import certificate for the root CA in the certification path of the Skype for Business certificate:

- 1** Using Windows explorer, on each of the trusted computers that will be hosting MiCollab AM call server(s), select the file containing the export of the certificate for the root CA in the certification path of the Skype for Business certificate.
- 2** Right-click on the certificate and select **Install Certificate** from the contextual menu.

- 3 In the opening page of the Windows certificate import wizard, select the **Local Machine** store location.
- 4 In the **Certificate Store** page, select the **Place all certificates in the following store and using the Browse** button.
- 5 Choose the **Trusted Root Certification Authorities** store.
- 6 After confirming the selections, on the last page, click the Finish button to complete the import operation.

Configuring Call Forwarding for Skype for Business Clients

Users with Skype for Business basic version client will not be able to set directly their call forwarding options. They cannot forward unanswered calls to MiCollab AM.

In this scenario, you can use **Secondary Extension Feature Activation Utility (SEFAUtil)** to configure call forwarding.

You can get detailed information about how to install this tool and how to use it to configure call forwarding options from the Microsoft website: technet.microsoft.com/en-us/library/jj945659.aspx

This section briefly describes the steps taken in order to use this tool to configure call forwarding.

To configure call forwarding using SEFAUtil.exe:

- 1 Download and install SEFAUtil from the Microsoft website.
- 2 Configure SEFAUtil as a trusted application. This process is very similar to the process described above for configuring MiCollab AM as a trusted application. For more information about deploying the SEFAUtil tool in Skype for Business, see: technet.microsoft.com/en-us/library/jj945659.aspx
- 3 Once the application is installed and configured, you can use it from the command line or PowerShell to configure call forwarding. The following is an example of configuring forward unanswered calls to the MiCollab AM trusted application configured above:

```
SEFAUtil.exe /server:SFB.sfbdomain.local sip:jsmith@sfbdomain.local  
/enablefwdnoanswer /callanswerwaittime:20 /setfwddestination:1600@  
sfbdomain.local
```

Table 11. Call Forwarding Configuration for Skype for Business Client

Argument	Description
server	Skype for Business Server FQDN, required if auto-discovery is not enabled
enablefwdnoanswer	Sets user's call handling rules to forward unanswered calls to forward destination
setfwddestination	Sets the user's Forward All or Forward No Answer destination

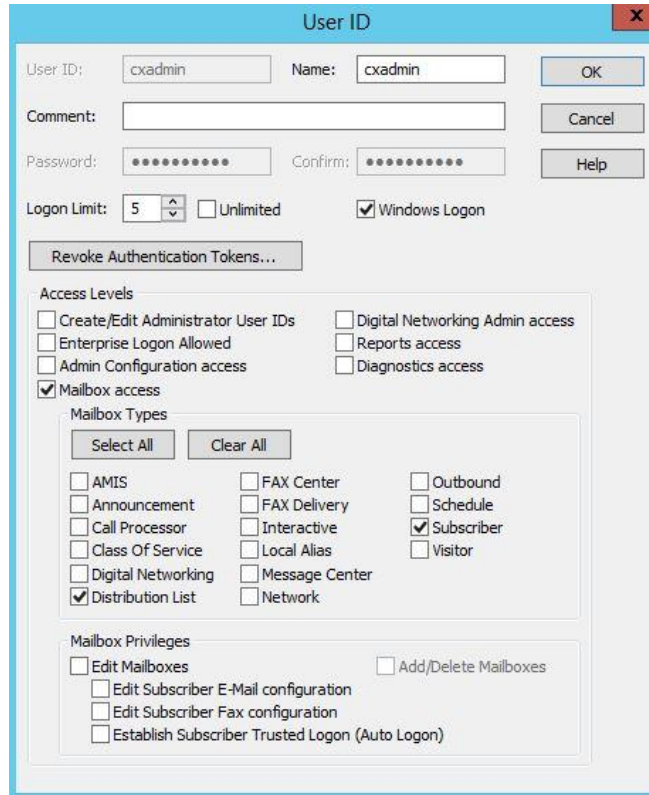
Skype for Business cannot be configured for **Call Forward Busy** or **Call Forward DND** but it is possible to work around this with the **Skype for Business Routing on Busy** application. **Skype for Business Routing on Busy** is an application that installs on Skype for Business Front End server. When this application is installed, calls will be automatically forwarded when the following call scenarios are set on Skype for Business clients: DND, Presenting, Busy, or On the Phone. Once MiCollab AM receives the call, normal MiCollab AM call processing engages and tells the caller that the user is busy or on the phone, and can optionally play the busy greeting. The **Skype for Business Routing on Busy** script can be found under the MiCollab AM installation folder **\Utilities\SfB Routing on Busy\InstallRoutingOnBusyService.ps1**

NOTE The service must be installed on all Front End servers where MiCollab AM users log on with their Skype for Business clients.

Prerequisites:

The following prerequisites must be met prior to beginning the installation process.

- 1** A Windows account with the right to "Log on as a service" on all Front End servers where the application will be installed. This account needs to have permission to create folders and files in the location where the application will be installed.
- 2** This account must be a read-only Skype for Business administrator in order to download required information. It uses the following PowerShell commands to retrieve information:
Get-CSUser – To retrieve the SIP addresses and their associated LineURI
Get-CSDialPlan – To retrieve the list of dial plans and the normalization rules defined in these plans. The normalization rules are used to translate the CX extensions to LineURIs.
- 3** The same Windows account must be configured as MiCollab AM administrator. It does not need "Edit Mailboxes" rights. The application will use this account to connect to MiCollab AM and download information about the MiCollab AM users. It retrieves for each user the extensions defined on the switch sections configured for any Microsoft switch. These extensions are translated to LineURI using the normalization rules of the configured dial plan. The obtained LineURI is used to map CX users to the Skype for Business accounts.



The image shows a 'User ID' configuration window. It contains fields for 'User ID' (cxadmin), 'Name' (cxadmin), 'Comment', 'Password', and 'Confirm'. There are 'OK', 'Cancel', and 'Help' buttons. Below these are 'Logon Limit' (set to 5) and 'Windows Logon' (checked). A 'Revoke Authentication Tokens...' button is present. The 'Access Levels' section includes checkboxes for 'Create/Edit Administrator User IDs', 'Enterprise Logon Allowed', 'Admin Configuration access', 'Mailbox access' (checked), 'Digital Networking Admin access', 'Reports access', and 'Diagnostics access'. The 'Mailbox Types' section has 'Select All' and 'Clear All' buttons, followed by checkboxes for various mailbox types: AMIS, Announcement, Call Processor, Class Of Service, Digital Networking, Distribution List (checked), FAX Center, FAX Delivery, Interactive, Local Alias, Message Center, Network, Outbound, Schedule, Subscriber (checked), and Visitor. The 'Mailbox Privileges' section includes checkboxes for 'Edit Mailboxes', 'Add/Delete Mailboxes', 'Edit Subscriber E-Mail configuration', 'Edit Subscriber Fax configuration', and 'Establish Subscriber Trusted Logon (Auto Logon)'.

To configure Call Forward Busy using Skype for Business Routing on Busy application:

- 1 Copy the entire "SfB Routing on Busy" folder to a network location that can be easily accessed from all Front End servers.
- 2 Type the script path in PowerShell or the **Skype for Business Management Shell** instance and execute the script **InstallRoutingOnBusyService.ps1**

NOTE The script must be executed with elevated privileges in order to register the new service with the Service Control Manager. In addition, the account used for the installation must be a Skype for Business administrator that has the rights to execute the following PowerShell commands:

Get-CSTrustedApplicationEndpoint
Get-CSDialPlan
Get-CSServerApplication
New-CSServerApplication

- 3 The installation utility dialog box appears.

SfB routing on busy: installation utility

Target location [Location where application files will be copied]
 ...

Voicemail server FQDN: SOAP Port:

☐ Use secure connection
Note: This will work only with the appropriate SOAP port on the voicemail server - usually 18277

Windows account for the service [it must include the domain]:

Note: This account should also be a voicemail administrator. It does not require mailbox edit rights.

Password: Confirm password:


Voicemail Contact End Point:

Voicemail Dial Plan:

Routing Rules:
☒ Route on BUSY and DND
☐ Route only on BUSY
☐ Route only on DND

Install

- 4 Specify the location where the files of the application will be copied in the **Target location** field. The Windows service for the application will be configured to run from this application.

NOTE The script will create the sub-folders in the path that do not exist. It will copy the files in the specified location and will not automatically create any sub-folders. Use the  browse button to create and select this path.

- 5 Specify the fully qualified domain name of the MiCollab AM system server in the **Voicemail server FQDN** field.
- 6 Specify the TCP port that the MiCollab AM system server is using for listening for SOAP requests in the **SOAP Port** field. The default value is 18276. In case the MiCollab AM system was configured to use a different port, the configured value must be provided here.
- 7 Select the **Use secure connection** checkbox to have the SOAP communication with MiCollab AM system carried over a TLS connection. This step is optional.

NOTE The MiCollab AM SOAP Port must be set to the port where MiCollab AM is listening for TLS connections. The default port is 18277.

- 8 Specify the Windows account prepared as specified in prerequisites in the **Windows account for the service** field.

NOTE: The account must include the domain.

- 9 Enter the password for the account specified above in the **Password** field.
- 10 Enter the password for the account specified above in the **Confirm password** field.

- 11 The **Voicemail Contact End Point** box is populated with the list of all trusted application end points defined on the Skype for Business deployment. Please select the one configured for MiCollab AM.

NOTE The application will use the SIP address associated with this endpoint to route the calls that are targeting a user that is in Busy or DND.

- 12 The **Voicemail Dial Plan** box is populated with the list of all dial plans defined in the Skype for Business deployment. Select the voicemail dial plan configured for MiCollab AM.

NOTE The application will use the normalization rules associated with this dial plan in order to translate the MiCollab AM extensions to LineURIs. The Line URI is the link between MiCollab AM mailboxes and Skype for Business accounts.

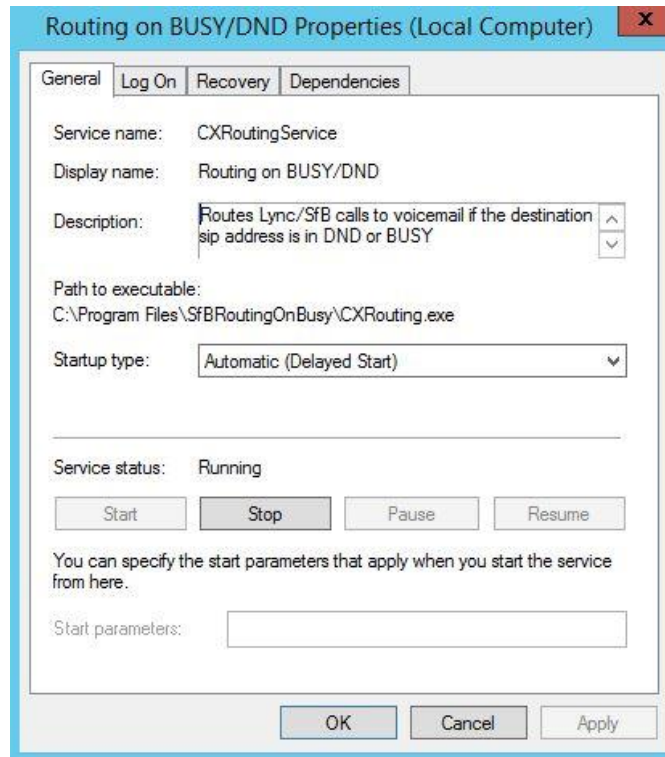
- 13 Select the appropriate check box in the **Routing Rules** area. This setting configures the scenarios in which the application will route calls to MiCollab AM:

- **Route on BUSY and DND** – MiCollab AM will route calls that are targeting a Skype for Business subscriber whose client is either in busy or DND.
- **Route only on BUSY** – MiCollab AM will route calls that are targeting a Skype for Business subscriber whose client is busy.
- **Route only on DND** – MiCollab AM will route calls that are targeting a Skype for Business subscriber whose client is in DND.

- 14 Click **Install**. After clicking the **Install** button, the script will:

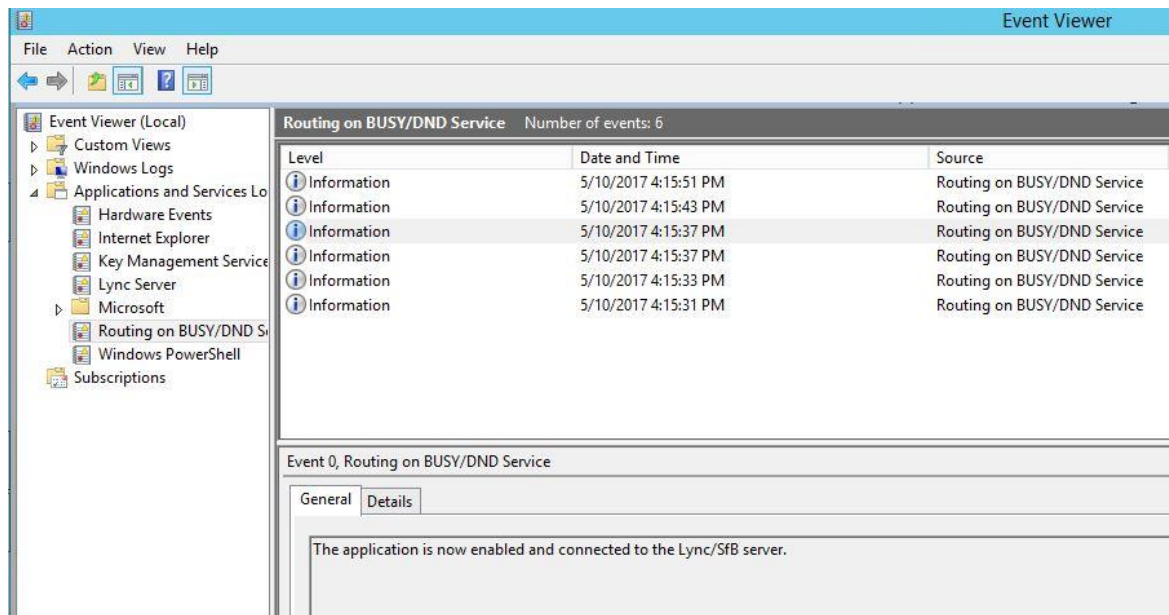
- Create the specified target location.
- Extract the files to the target location.
- Save the settings to the configuration file for the application.
- Register the service "CXRoutingService" with the Service Control Manager using the display name "Routing on Busy/DND".
- Register the application as a Skype for Business application using the New-CSServerApplication PowerShell command.
- Add the specified account to the local group "RTC Server Applications" in order to communicate with the Skype for Business server.
- Creates a custom Windows log "Routing on Busy/DND" for the events generated by this application.

- 15 Open the **Service Control Manager** and verify that the service is started successfully.



- 16 After starting the service, check the event viewer for any issues. The new service is logging event entries to the "Routing on Busy/DND" log, which in event viewer will be located under the "Applications and Services Logs". A successful startup will log the following events:

The application is now enabled and connected to the Lync/SfB server.



NOTE It takes some time for the Skype for Business to enable the new server application. For this reason, right after the installation, the application might fail to connect to the server. The application will log an entry and will re-attempt the connection. For example:

Successfully downloaded initial SfB information.

Successfully downloaded initial information for MiCollab AM mailboxes.

NOTES

1. The application uses the SIP response messages sent by the clients to update the internal status for client. Because of this, the application will not have the initial state of the Skype for Business clients after the service is started. Until the status is updated, the application might allow calls to go to users that have status in busy or DND. A possible work around for this issue is to restart the Skype for Business RTC service. However, this takes a few minutes and the functionality of Skype for Business will be impaired during that period.
2. Because the Skype for Business clients send status messages only to the Front End server where they are registered, the application will be able to monitor only the accounts registered on the Front End server where it was installed. Therefore, installing it on all Front End servers ensures that all accounts are being monitored.
3. The application uses the highest availability number determined by the Skype for Business server. Because of this, the calls from users in the colleagues groups will be routed to MiCollab AM when they attempt to call a user that has status in DND.
4. Every time the application refreshes the information for Skype for Business accounts and MiCollab AM mailboxes, it also reads the content of the "excludedSipAddresses.in", if it exists. By default, the refresh cycle starts every 5 minutes. The content of the special file "excludedSipAddresses.in" is a list of SIP addresses that are associated with MiCollab AM mailboxes but for any reason should not be monitored. Calls targeting these addresses will never be routed to MiCollab AM regardless of the status of the Skype for Business client.

Configuring MiCollab AM

Once the telephone system is programmed, you must configure MiCollab AM for the integration. There are two ways you can configure MiCollab AM:

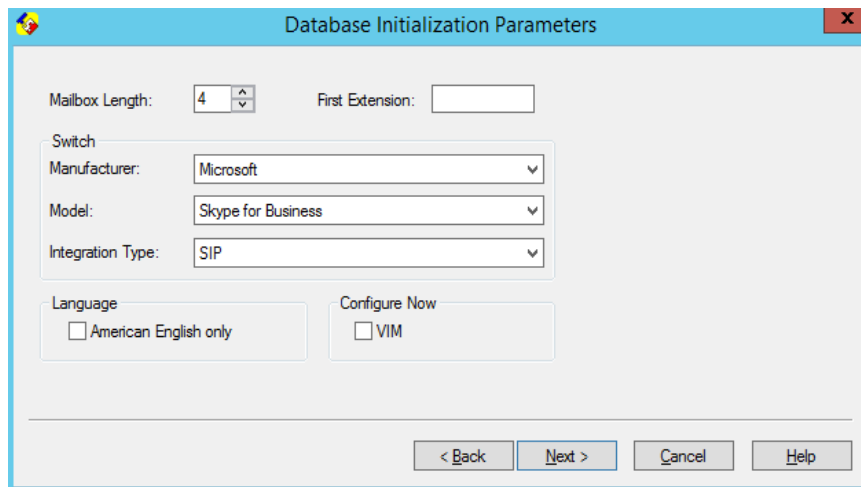
- [Configuring MiCollab AM for the Integration During Initial Installation](#): Integrate the telephone system while you install MiCollab AM for the first time.
- [Configuring Existing MiCollab AM for the Integration](#): Integrate a new telephone system on your existing MiCollab AM system.

NOTE For general information on integrations, see the **Integrating MiCollab AM with the Telephone System** chapter in the *System Installation and Configuration Guide*, and the topic, **Integrating MiCollab AM with the Telephone System**, in the online help.

Configuring MiCollab AM for the Integration During Initial Installation

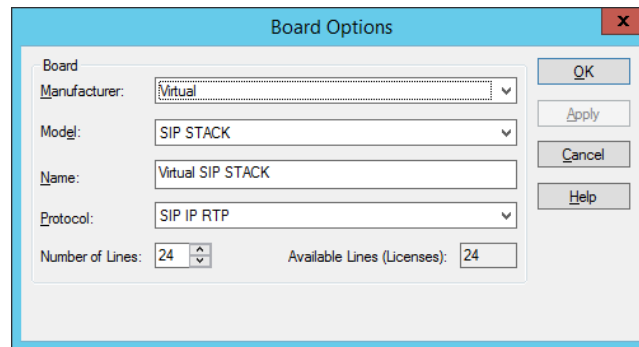
To configure MiCollab AM with the integration during the initial installation:

- 1 In the **Database Initialization Parameters** dialog box, configure the following options:



- a In the **Mailbox Length** box, enter the mailbox length in digits.
- b In the **First Extension** box, enter first extension number for the first line. You can also leave the **First Extension** box empty.
- c From the **Manufacturer** drop-down list, select **Microsoft**.
- d From the **Model** drop-down list, select **Skype for Business**.
- e From the **Integration Type** drop-down list, select **SIP**.

- 2 Click **Next**. The **Board Options** dialog box displays for the virtual board configuration.

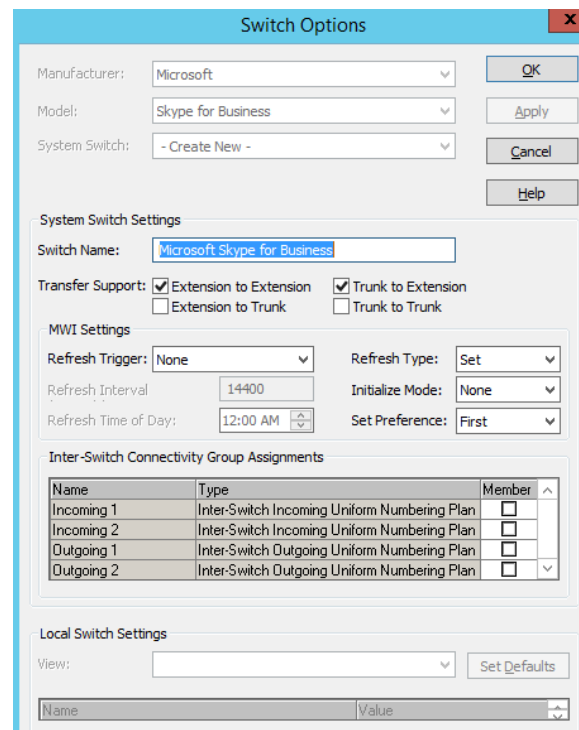


The **Board Options** dialog box is shown with the following settings:

- Manufacturer:** Virtual
- Model:** SIP STACK
- Name:** Virtual SIP STACK
- Protocol:** SIP IP RTP
- Number of Lines:** 24
- Available Lines (Licenses):** 24

Buttons on the right: OK, Apply, Cancel, Help.

- 3 In the **Board Options** dialog box, configure the following options:
- a From the **Manufacturer** drop-down list, select **Virtual**.
 - b From the **Model** drop-down list, select **SIP STACK**.
 - c In the **Name** field, the name for this board is automatically generated. Enter a new name if necessary.
 - d From the **Protocol** drop-down list, select **SIP IP RTP**.
 - e In the **Number of Lines** field, enter the number of lines this board uses. The total number of lines is limited by the capacity of the board and the number of **Available Line Licenses**.
- 4 Click **OK**. The **Switch Options** dialog box appears.



The **Switch Options** dialog box is shown with the following settings:

- Manufacturer:** Microsoft
- Model:** Skype for Business
- System Switch:** - Create New -
- System Switch Settings**
 - Switch Name:** Microsoft Skype for Business
 - Transfer Support:**
 - ☒ Extension to Extension
 - ☐ Extension to Trunk
 - ☒ Trunk to Extension
 - ☐ Trunk to Trunk
 - MWI Settings**
 - Refresh Trigger:** None
 - Refresh Interval:** 14400
 - Refresh Time of Day:** 12:00 AM
 - Refresh Type:** Set
 - Initialize Mode:** None
 - Set Preference:** First
- Inter-Switch Connectivity Group Assignments**

Name	Type	Member
Incoming 1	Inter-Switch Incoming Uniform Numbering Plan	<input type="checkbox"/>
Incoming 2	Inter-Switch Incoming Uniform Numbering Plan	<input type="checkbox"/>
Outgoing 1	Inter-Switch Outgoing Uniform Numbering Plan	<input type="checkbox"/>
Outgoing 2	Inter-Switch Outgoing Uniform Numbering Plan	<input type="checkbox"/>
- Local Switch Settings**
 - View:** [Empty]
 - Set Defaults** button
 - Name** and **Value** fields

Buttons on the right: OK, Apply, Cancel, Help.

- 5 If necessary, make any changes to the default settings your site requires in the **Switch Options** dialog box.

NOTE The settings related to the telephone system in the **Switch Options** dialog box are filled in automatically when you select the correct telephone system during setup.

If you need to customize settings on the **Switch Options** dialog box to meet requirements specific to your site, see the documentation accompanying the telephone system, the online help, and the *System Installation and Configuration Guide*.

- 6 Click **OK**. The **Integration Options** dialog box appears.

Name	Value
SIP Server Address	
SIP Server Port	5061
SIP Domain Name	
Transport for outgoing SIP messages	TLS
Local IP Address to bind on	- Please Select -
SIP Local Connection Port	5060
SIP parser qualifier string	
Enable SIP Gateway Mode	<input type="checkbox"/>
Enable ICE	<input checked="" type="checkbox"/>

- 7 In the **Integration Options** dialog box, configure the following options:

- a Click the **Import** button to import the settings from the configuration file generated using the **Skype for Business integration configurator** script.
- In the **Open** dialog box, select the configuration, and then click **Open**.
 - Once the file is selected, the MiCollab AM configuration tool will parse the data from the file and overwrite the display value of the configuration data for current integration. In order for the changes to be saved, you must click the **OK** or **Apply** button.

NOTE If the configuration data contains the certificate for the MiCollab AM call server, you will be prompted to provide the export password. This password was specified when exporting the MiCollab AM call server(s) data using the configuration script.

If the certificate for the trusted application exists in the configuration import file and a valid password is provided, the MiCollab AM system configuration application will import the certificate into the Windows personal certificates store for local computer. If the root in the certificates chain of the Skype for Business server certificate exists in the configuration import file, the MiCollab AM system configuration application will import this certificate into the Windows trusted root certificates store.

- b In the **Local Integration Settings** section, select the **Required Parameters** view, and configure the settings as follows:

NOTE Detailed information about the MiCollab AM integration parameters that must be configured in order to enable MiCollab AM call server(s) to communicate with Skype for Business and Skype for Business clients are presented in a later section of this document.

Table 12. Required Parameters View – Integration Options

Field	Value
SIP Server Address	<p>Skype for Business Standard Edition: Enter the FQDN of the Skype for Business Standard Edition Front End server</p> <p>Skype for Business Enterprise Edition: Enter the FQDN of the Skype for Business Enterprise Edition Front End pool.</p> <p>IMPORTANT The value should match the name defined in the <i>Subject</i> field of the certificate for Skype for Business and cannot be any of the DNS names in the <i>Subject Alternative Name</i>.</p> <p>NOTE The value is case sensitive and must match the name defined in the <i>Subject</i> field of the certificate for Skype for Business.</p>
SIP Domain Name	<p>Enter the domain name in which the Skype for Business Server resides.</p> <p>NOTE This value is case-sensitive.</p>
Transport for outgoing SIP Messages	Select TLS as the transport.
Local IP Address to bind on	Select the IP address of the NIC on the Call Server platform that communicates with the Skype for Business Server. The drop-down box displays all available local IP addresses.
SIP parser qualifier string	Enter the FQDN of the trusted application pool you created for MiCollab AM.
Enable SIP Gateway Mode	Check this only if planning to use the integration as a gateway to another PBX. Refer to the Enabling Gateway Support section.
Enable ICE	Must be checked .
Computer GRUU	<p>GRUU value generated by Skype for Business Server when the computer was added to the trusted application pool.</p> <p>NOTE The GRUU can be retrieved by running the <i>Get-CsTrustedApplication</i> command. This command displays detailed information about all trusted applications. The administrator should identify the trusted application</p>

created for MiCollab AM and check the *ComputerGruus* list for that trusted application as shown in the example below.

```
Identity : cx-trusted-apps.sfbdomain.local/urn:application:cx-voicemail
ComputerGruus : {CS1.sfbdomain.local sip:CS1.sfbdomain.local@sfbdomain.local;
gruu:opaque=svr:cx-voicemail:PjrEwmr_01Ct9h-11wQHaQAA}
ServiceGruu : sip:cx-trusted-apps.sfbdomain.local@sfbdomain.local;gruu:opaque=svr:cx-voicemail:bEG3ESpZ110u1m6mYej8hAAA
Protocol : Mtls
ApplicationId : urn:application:cx-voicemail
TrustedApplicationPoolFqdn : cx-trusted-apps.sfbdomain.local
Port : 5061
LegacyApplicationName : cx-voicemail
```

Each entry in the *ComputerGruus* list is the address of a trusted computer followed by the generated GRUU. The appropriate GRUU should be selected for the Call Server computer

IMPORTANT The *sip:* prefix is part of the *ComputerGRUU* and is required.

- c** In the **Local Integration Settings** section, select the **Integration Specific Parameters** View, and configure the following options:

Table 13. Integration Specific Parameters for Integration Options

Field	Value
Template for phone-context parameter	Enter the simple name of the dial plan that MiCollab AM should use when dialing.
Use Single Channel for Monitored Transfers	Make sure this option is unchecked .
Use DNS discovery procedures	Make sure this option is unchecked .

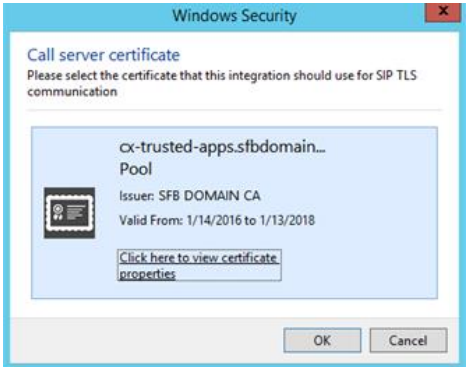
- d** In the **Local Integration Settings** section, select the **Connection Security Settings** View, and configure the following options:

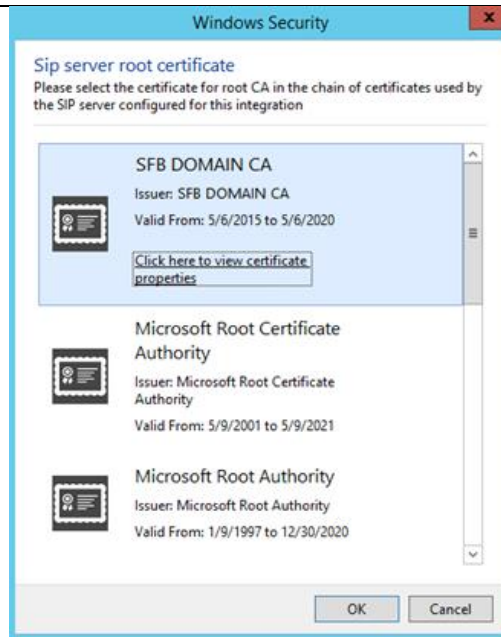
NOTE If you are having trouble using the certificates from the Windows certificates store, then you can configure MiCollab AM to use the certificate files directly.

Refer to [Appendix B – Configuring MiCollab AM to Use Certificate Files Directly](#) for more detailed instructions.

Table 14. Connection Security Settings

Field	Value
Enable TLS	This parameter must be checked .
SIP Server Address	<p>Skype for Business Standard Edition: Enter the IP or FQDN of the Skype for Business Standard Edition Front End server.</p> <p>Skype for Business Enterprise Edition: Enter the IP or FQDN of all the Skype for Business Enterprise Edition Front End servers in the pool.</p> <p>NOTE You need to click the Add Trusted SIP Server Address button for a SIP Server Address entry to be created. You must enter the IP/FDQN of all the Skype for Business Front End servers if you have Skype for Business Enterprise Edition with multiple front end servers deployed in your environment.</p>
SIP server TLS Port	<p>Enter network port number used by Skype for Business Front End Server for SIP TLS connections.</p> <p>NOTE To determine this value you can execute the following cmdlet in PowerShell: <i>Get-CsService -Registrar</i></p>

	The <i>SipPort</i> field reported by the command is the value required for this parameter
SIP Local TLS Port	Enter the port number assigned when MiCollab AM was registered as a trusted application through the PowerShell cmdlet <i>New-CsTrustedApplication</i> .
SSL/TLS protocol version	Select the SSL/TLS protocol version to be used. NOTE To create secure connections, use TLS 1.3 (recommended where available) or 1.2 for the System Server and Call Servers.
Override list of ciphers to use	Specify the ciphers or cipher suites to be used for your integration in Open SSL format. For example, if SHA1+DES is specified then all cipher suites containing the SHA1 and DES algorithms will be used. NOTE This parameter is empty by default which means all ciphers will be used.
Thumbprint call server certificate	Use the browse (...) button to open the Windows select certificate wizard that will present a list with all certificates from the Personal folder of Windows certificates store for the local computer.  <p>Select the MiCollab AM trusted application certificate and click OK.</p> <p>For more details about generating and importing the certificate into the Windows certificates store of the computer hosting the call server, see Importing Certificates into the Computer Hosting the MiCollab AM Call Server section.</p>
Thumbprint remote root CA certificate	Use the browse (...) button to open the Windows select certificate wizard that will present a list with all certificates from the Trusted Root Certification Authorities folder of the Windows certificates store for the local computer.



Select the certificate for the root CA in the certification path of the Skype for Business certificate and then click **OK**.

For more details about generating and importing the certificate into the Windows certificates store of the computer hosting the call server, see [Importing Certificates into the Computer Hosting the MiCollab AM Call Server](#) section.

-
- 8 Click **OK**. The **Switch Section Options** dialog box appears.

Switch Section Options

Local Switch: Microsoft Skype for Business

System Switch Section: - Create New -

System Switch Section Settings

Name: Microsoft Skype for Business Section

Node Code:

Location Code:

Location: Seattle

MWI Integration: Microsoft Skype for Business SIP

Local Switch Section Settings

View: Required Parameters

Set Defaults

Name	Value
Incoming Hunt Mode	Terminal
Hunt Group Access Code	

- 9 In the **Switch Section Options** dialog box, configure the following options:
 - a In the **Local Switch Section Settings** section, select the **Required Parameters** View.
 - b In **Incoming Hunt Mode**, select **Terminal**.
 - c In **Hunt Group Access Code** box, type the telephone number (pilot number) for this integration.
 - d Click **OK**.
- 10 Continue through and complete the configuration. At the end of the configuration, a confirmation dialog box appears. Click **OK**.
- 11 If **MiCollab AM Configuration** does not open automatically after the configuration completes, open **MiCollab AM Configuration**, and select the **Lines** tab.
- 12 In the table from the **Lines** tab, enter the extension number of each integrated line on the Call Server.
- 13 Click **OK** to save all changes.

Configuring Existing MiCollab AM for the Integration

To configure exiting MiCollab AM for the telephone integration:

- 1 Open **MiCollab AM Configuration**, and go to the **Main** tab.

- 2 In the **Main** tab, click **Shutdown** to stop the system. Wait until the **Current Status** shows **Stopped**.

NOTE If you have not configured the virtual board with your MiCollab AM system yet, complete **Step 3**. If your MiCollab AM already has the virtual board configured, skip to **Step 4**.

- 3 **[Optional]** Select the **Boards** tab, and then click the **Add** button. The **Board Options** dialog box appears.

- a From the **Manufacturer** drop-down list, select **Virtual**.
 - b From the **Model** drop-down list, select **SIP STACK**.
 - c In the **Name** field, the name for this board is automatically generated. Enter a new name if necessary.
 - d From the **Protocol** drop-down list, select **SIP IP RTP**.
 - e In the **Number of Lines** field, enter the number of lines this board uses. The total number of lines is limited by the capacity of the board and the number of **Available Line Licenses**.
 - f Click **OK**.
- 4 Select the **Switch** tab, and click the **Add** button. The **Switch Integration Data Setup** dialog box appears.

- a From the **Manufacturer** drop-down list, select **Microsoft**.
 - b From the **Model** drop-down list, select **Skype for Business**.
 - c From the **Integration Type** drop-down list, select **SIP**.
- 5 Click **OK**. The **Switch Options** dialog box appears.

Switch Options

Manufacturer:

Model:

System Switch:

System Switch Settings

Switch Name:

Transfer Support: ☒ Extension to Extension ☒ Trunk to Extension
☐ Extension to Trunk ☐ Trunk to Trunk

MWI Settings

Refresh Trigger: Refresh Type:
Refresh Interval: Initialize Mode:
Refresh Time of Day: Set Preference:

Inter-Switch Connectivity Group Assignments

Name	Type	Member
Incoming 1	Inter-Switch Incoming Uniform Numbering Plan	<input type="checkbox"/>
Incoming 2	Inter-Switch Incoming Uniform Numbering Plan	<input type="checkbox"/>
Outgoing 1	Inter-Switch Outgoing Uniform Numbering Plan	<input type="checkbox"/>
Outgoing 2	Inter-Switch Outgoing Uniform Numbering Plan	<input type="checkbox"/>

Local Switch Settings

View:

Name	Value

- 6 If necessary, make any changes to the default settings your site requires in the **Switch Options** dialog box.

NOTE The settings related to the telephone system in the **Switch Options** dialog box are filled in automatically when you select the correct telephone system during setup.

If you need to customize settings on the **Switch Options** dialog box to meet requirements specific to your site, see the documentation accompanying the telephone system, the online help, and the *System Installation and Configuration Guide*.

- 7 Click **OK**. The **Integration Options** dialog box appears.

Name	Value
SIP Server Address	
SIP Server Port	5061
SIP Domain Name	
Transport for outgoing SIP messages	TLS
Local IP Address to bind on	- Please Select -
SIP Local Connection Port	5060
SIP parser qualifier string	
Enable SIP Gateway Mode	<input type="checkbox"/>
Enable ICE	<input checked="" type="checkbox"/>

8 In the **Integration Options** dialog box, configure the following options:

- a Click the **Import** button to import the settings from the configuration file generated using the **Skype for Business integration configurator** script.
 - In the **Open** dialog box, select the configuration, and then click **Open**.
 - Once the file is selected, the MiCollab AM configuration tool will parse the data from the file and overwrite the display value of the configuration data for current integration. In order for the changes to be saved, you must click the **OK** or **Apply** button.

NOTE If the configuration data contains the certificate for the MiCollab AM call server, you will be prompted to provide the export password. This password was specified when exporting the MiCollab AM call server(s) data using the configuration script.

If the certificate for the trusted application exists in the configuration import file and a valid password is provided, the MiCollab AM system configuration application will import the certificate into the Windows personal certificates store for local computer.

If the root in the certificates chain of the Skype for Business server certificate exists in the configuration import file, the MiCollab AM system configuration application will import this certificate into the Windows trusted root certificates store.

- b In the **Local Integration Settings** section, select the **Required Parameters** view, and configure the settings as follows:

NOTE Detailed information about the MiCollab AM integration parameters that must be configured in order to enable MiCollab AM call server(s) to communicate with Skype for Business and Skype for Business clients are presented in a later section of this document.

Table 15. Required Parameters View – Integration Options

Field	Value
SIP Server Address	<p>Skype for Business Standard Edition: Enter the FQDN of the Skype for Business Standard Edition Front End server</p> <p>Skype for Business Enterprise Edition: Enter the FQDN of the Skype for Business Enterprise Edition Front End pool.</p> <p>IMPORTANT The value should match the name defined in the <i>Subject</i> field of the certificate for Skype for Business and cannot be any of the DNS names in the <i>Subject Alternative Name</i>.</p> <p>NOTE The value is case sensitive and must match the name defined in the <i>Subject</i> field of the certificate for Skype for Business.</p>
SIP Domain Name	<p>Enter the domain name in which the Skype for Business Server resides.</p> <p>NOTE This value is case-sensitive.</p>
Transport for outgoing SIP Messages	Select TLS as the transport.
Local IP Address to bind on	Select the IP address of the NIC on the Call Server platform that communicates with the Skype for Business Server. The drop-down box displays all available local IP addresses.
SIP parser qualifier string	Enter the FQDN of the trusted application pool you created for MiCollab AM.
Enable SIP Gateway Mode	Check this only if planning to use the integration as a gateway to another PBX. Refer to the Enabling Gateway Support section.
Enable ICE	Must be checked .
Computer GRUU	<p>GRUU value generated by Skype for Business Server when the computer was added to the trusted application pool.</p> <p>NOTE The GRUU can be retrieved by running the <i>Get-CsTrustedApplication</i> command. This command displays detailed information about all trusted applications. The administrator should identify the trusted application created for MiCollab AM and check the <i>ComputerGruus</i> list for that trusted application as shown in the example below.</p>

```

Identity          : cx-trusted-aops.sfbdomain.local/urn:application:cx-voicemail
ComputerGruus    : {CS1.sfbdomain.local sip:CS1.sfbdomain.local@sfbdomain.local;
                   gru;opaque=svr:cx-voicemail:PjEwmm_01Ct9h-11wQHaQAA}
ServiceGruu      : sip:cx-trusted-apps.sfbdomain.local@sfbdomain.local;gru;opaq
                   ue=svr:cx-voicemail:bEG3Espz110u7m6mYej8hAAA
Protocol         : Mtls
ApplicationId     : urn:application:cx-voicemail
TrustedApplicationPoolFqdn : cx-trusted-apps.sfbdomain.local
Port             : 5061
LegacyApplicationName : cx-voicemail

```

Each entry in the *ComputerGruus* list is the address of a trusted computer followed by the generated GRUU. The appropriate GRUU should be selected for the Call Server computer

IMPORTANT The *sip:* prefix is part of the *ComputerGRUU* and is required.

- c** In the **Local Integration Settings** section, select the **Integration Specific Parameters** View, and configure the following options:

Table 16. Integration Specific Parameters for Integration Options

Field	Value
Template for phone-context parameter	Enter the simple name of the dial plan that MiCollab AM should use when dialing.
Use Single Channel for Monitored Transfers	Make sure this option is unchecked .
Use DNS discovery procedures	Make sure this option is unchecked .

- d** In the **Local Integration Settings** section, select the **Connection Security Settings** View, and configure the following options:

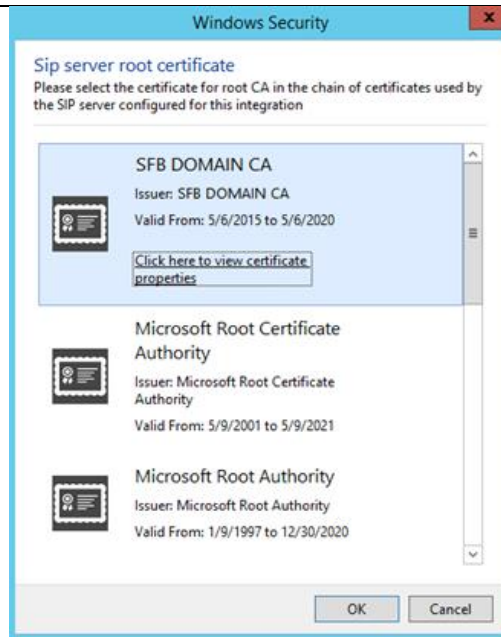
NOTE If you are having trouble using the certificates from the Windows certificates store, then you can configure MiCollab AM to use the certificate files directly.

Refer to [Appendix B – Configuring MiCollab AM to Use Certificate Files Directly](#) for more detailed instructions.

Table 17. Connection Security Settings

Field	Value
Enable TLS	This parameter must be checked .
SIP Server Address	<p>Skype for Business Standard Edition: Enter the IP or FQDN of the Skype for Business Standard Edition Front End server.</p> <p>Skype for Business Enterprise Edition: Enter the IP or FQDN of all the Skype for Business Enterprise Edition Front End servers in the pool.</p> <p>NOTE You need to click the Add Trusted SIP Server Address button for a SIP Server Address entry to be created. You must enter the IP/FDQN of all the Skype for Business Front End servers if you have Skype for Business Enterprise Edition with multiple front end servers deployed in your environment.</p>
SIP server TLS Port	<p>Enter network port number used by Skype for Business Front End Server for SIP TLS connections.</p> <p>NOTE To determine this value you can execute the following cmdlet in PowerShell: <i>Get-CsService -Registrar</i> The <i>SipPort</i> field reported by the command is the value required for this parameter</p>

SIP Local TLS Port	Enter the port number assigned when MiCollab AM was registered as a trusted application through the PowerShell cmdlet <i>New-CsTrustedApplication</i> .
SSL/TLS protocol version	<p>Select the SSL/TLS protocol version to be used.</p> <p>NOTE It is recommended to use TLS 1.2 or higher to create secure connections.</p>
Override list of ciphers to use	<p>Specify the ciphers or cipher suites to be used for your integration in Open SSL format. For example, if SHA1+DES is specified then all cipher suites containing the SHA1 and DES algorithms will be used.</p> <p>NOTE This parameter is empty by default which means all ciphers will be used.</p>
Thumbprint call server certificate	<p>Use the browse (...) button to open the Windows select certificate wizard that will present a list with all certificates from the Personal folder of Windows certificates store for the local computer.</p> <div data-bbox="786 894 1242 1260" data-label="Image"> </div> <p>Select the MiCollab AM trusted application certificate and click OK.</p> <p>For more details about generating and importing the certificate into the Windows certificates store of the computer hosting the call server, see Importing Certificates into the Computer Hosting the MiCollab AM Call Server section.</p>
Thumbprint remote root CA certificate	Use the browse (...) button to open the Windows select certificate wizard that will present a list with all certificates from the Trusted Root Certification Authorities folder of the Windows certificates store for the local computer.



Select the certificate for the root CA in the certification path of the Skype for Business certificate and then click **OK**.

For more details about generating and importing the certificate into the Windows certificates store of the computer hosting the call server, see [Importing Certificates into the Computer Hosting the MiCollab AM Call Server](#) section.

- 9 Click **OK**. The **Switch Section Options** dialog box appears.

Switch Section Options

Local Switch: Microsoft Skype for Business

System Switch Section: - Create New -

System Switch Section Settings

Name: Microsoft Skype for Business Section

Node Code:

Location Code:

Location: Seattle

MWI Integration: Microsoft Skype for Business SIP

Local Switch Section Settings

View: Required Parameters

Set Defaults

Name	Value
Incoming Hunt Mode	Terminal
Hunt Group Access Code	

- 10 In the **Switch Section Options** dialog box, configure the following options:
 - a In the **Local Switch Section Settings** section, select the **Required Parameters** View.
 - b In **Incoming Hunt Mode**, select **Terminal**.
 - c In **Hunt Group Access Code** box, type the telephone number (pilot number) for this integration.
 - d Click **OK**.
- 11 In **MiCollab AM Configuration**, verify that the telephone system is properly added and configured in the **Switches**, **Switch Sections**, and **Integrations** tabs.
- 12 Select the **Lines** tab.
- 13 In the table from the **Lines** tab, configure callouts for the application. For information on configuring callout settings, see the topic *Configuring Callout Settings*, in the online help system.
- 14 Click **OK** to save all changes.

Configuring the Extension Device for Subscribers

You must add an extension device that matches the LineURI of the Skype for Business user and in which conforms to the Skype for Business Dial Plan/Normalization Rules.

To add an extension device to the subscriber's device:

- 1 Log on to **MiCollab AM Administration**, select a Subscriber Mailbox to edit, and then click the **Devices** tab.
- 2 On the **Devices** tab, under the **Devices List**, click **Add**.
- 3 In the **Add “Device”** dialog box, select **Extension** from the **Category** drop-down list, overwrite the Name if necessary, and then click **OK**. The **Extension Properties** become input-enabled.
- 4 In the **Properties**, add the subscriber extension device number in the **Number** field. In this example, the subscriber extension number is **1613**.

The screenshot shows the 'Add Device' dialog box in the MiCollab AM Administration interface. The 'Category' is set to 'Extension'. The 'Number/Username' field contains '1613'. The 'Type/Capabilities' is set to 'Phone: logon, can receive calls'. The 'Category' is set to 'Extension'. The 'Primary Device' checkbox is checked. The 'Ring Timeout (sec)' is set to 14. The 'Active' checkbox is checked. The 'Barge In Sensitivity' slider is set to 0. The 'Extension Properties' section shows 'MWI' is unchecked, 'Switch Section' is set to 'Microsoft Skype for Business Section', 'Direct Dial' is empty, 'SMDI Prefix' is empty, and 'Enable Fax Tone Detection' is unchecked.

NOTE If your client has only a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI), such as the Skype for Business Mac client or if you have Polycom phones and want to use MWI functionality, you should also configure a SIP URI device. For more information, refer to the procedure in [Configuring a SIP URI Extension Device for Subscribers](#).

- 5 Select the **Primary Device** check box to identify the extension as the primary extension.
- 6 Select the **Type/Capabilities** from the drop-down list.
- 7 Select the **Category Default** check box if this is the default device in this category of device types.
- 8 Select the **Switch Section** to which the device belongs (**Microsoft Lync 2013 Section** or **Microsoft Skype for Business**).
- 9 Enter the **Direct Dial** (DID) (DIL) telephone number of the subscriber (if applicable).
- 10 Click **OK**.

Configuring a SIP URI Extension Device for Subscribers

In addition to Extension Device, you must also configure a SIP URI Extension Device. If your client has only a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI), such as the Skype for Business Mac client or if you have Polycom phones and want to use MWI functionality.

NOTE Skype for Business Mac client version 16.18.51 or prior versions has only a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) therefore you should also configure a SIP URI device. You should only need to configure an extension device for Skype for Business Mac client version later than 16.18.51.

To add a SIP URI extension device to the subscriber's device:

- 1 Log on to **MiCollab AM Administration**, select a Subscriber Mailbox to edit, and then click the **Devices** tab.
- 2 On the **Devices** tab, under the **Devices List**, click **Add**.
- 3 In the **Add "Device"** dialog box, select **Extension** from the **Category** drop-down list, overwrite the Name if necessary. In this example, another Extension device has been added to the **Device List** and has been given the name *SIP URI Extension*.

The screenshot displays the 'Add Device' dialog box in the MiCollab AM Administration interface. The 'Device List' at the top shows two entries: 'Extension' and 'SIP URI Extension'. The 'Properties' section contains the following fields and options:

- Number/Username:** abc
- ☒ Treat value as a SIP Username
- Type/Capabilities:** Phone: logon, can receive calls
- Category:** Extension
- ☐ Category Default
- Mailboxes Sharing this Number:** (empty box)
- ☐ Primary Device
- ☐ Primary Mobile Device
- Ring Timeout (sec):** 14
- ☒ Active
- Barge In Sensitivity:** -3, 0, +5 (slider)
- ☒ MWI
- Switch Section:** Microsoft Skype for Business Section
- Direct Dial:** (empty box)
- SMDI Prefix:** (empty box)
- ☐ Enable Fax Tone Detection

- 4 Click **OK**. The **Extension Properties** become input-enabled.

- 5 In the **Properties** area, select the **Treat value as a SIP Username** check box and then add the Voice over IP (VoIP) user name in the **Number** field. In this example, the SIP URI address is abc@lmop.xyz, so the subscriber extension number that is entered into the **Number** field is *abc*.

NOTE You should only provide the name portion of a valid SIP URI address for the user.

- 6 Select the **Type/Capabilities** from the drop-down list.
- 7 In the **Extension Properties** section, select the **MWI** check box to enable the Message Waiting Indicator function for the extension.

NOTE This step is required to support MWI on Polycom phones.

- 8 Select the **Switch Section** to which the device belongs (**Microsoft Lync 2013 Section** or **Microsoft Skype for Business**).
- 9 Click **OK**.

Configuring MWI for Polycom Phones

To configure MWI for Polycom phones, you must configure the following:

- Extension Device for subscribers as described in the [Configuring the Extension Device for Subscribers](#) section.
- SIP URI Extension Device for subscribers as described in the [Configuring a SIP URI Extension Device for subscribers](#) section.
- Set the value of MWI interface method to MWI Message to Switch.
- Add e-mail address in the subscriber's user properties in active directory.

NOTE MWI is supported on Polycom CX500 and CX600 phones only.

To change the MWI interface method:

- 1 From **MiCollab AM Configuration**, click the **Integrations** tab.
- 2 From the **Integrations** list, select your integration, and then click **Edit**.
- 3 In the **Integration Options** dialog box, go to the **Local Integration Settings** section.
- 4 From the **View** drop-down list, select **Integration Specific Parameters**.
- 5 Scroll down to **MWI interface method** and change the value to **MWI Message to Switch**.

To add e-mail address to subscriber's user properties in active directory:

- 1 Open the **Active Directory User and Computers** snap-in located in **Administrative Tools**.
- 2 Open the properties page for the user (Right-click user and select **Properties**).
- 3 Select the **General** tab.

- 4 Enter the e-mail address of the user in the **E-mail** field. In this example, the e-mail address of the user is abc@lmop.xyz.

The screenshot shows a 'Test User Properties' dialog box with the following fields and values:

Field	Value
First name	Test
Initials	
Last name	User
Display name	Test User
Description	
Office	
Telephone number	
E-mail	abc@lmop.xyz
Web page	

Configuring MiCollab AM for SIP Failover

MiCollab AM can be configured for automatic failover to the secondary SIP server in the event of the primary/host SIP server failure. Use the instructions provided in this section to add or remove secondary SIP server(s) for failover.

To add a SIP failover server:

- 1 From **MiCollab AM Configuration**, click the **Integrations** tab.
- 2 From the **Integrations** list, select your integration, and then click **Edit**.
- 3 In the **Integration Options** dialog box, go to the **Local Integration Settings** section.
- 4 From the **View** drop-down list, select **Failover Server Settings**.
- 5 Click the **Add Failover Server** button. Two new rows are added to configure the secondary SIP server.
- 6 In the **Secondary SIP Server Address** and **Secondary SIP Server Port** rows, enter the appropriate value as follows:

Table 18. Secondary SIP Server Address and the Secondary SIP Server Port example

Field	Value
-------	-------

Secondary SIP Server Address Enter the TCP/IP address or an FQDN of the secondary node.

For example:

The IP address 123.45.6.789 as displayed on the Review/Modify SIP Gateway screen.

NOTE This integration requires the machine name to be a fully qualified domain name. Therefore, use the Machine Name field as displayed on the Review/Modify SIP Gateway screen during the integration process.

IMPORTANT This value must match the configuration on the Gateway of the secondary node.

Secondary SIP Server Port Enter the port number of the secondary node. The default value is **5060**.

7 From the **View** drop-down list, select **Integration Specific Parameters**. The **Integration Specific Parameters** view appears.

8 In the **Integration Specific Parameters** list, enter the information as shown in the following table:

NOTE The parameters in the following table is listed in alphabetical order. The actual Integration Specific Parameters on your system may not be listed in the same order presented in the table below.

Table 19. Integration Specific Parameters

Field	Value
Enable SIP server failover	Select this check box to allow for failover and to enable the failover server setting changes.
Delay (in ms) between Failover attempts	The delay in milliseconds before MiCollab AM attempts to register its port with the SIP server. The default is 1000 ms.
Incoming off hook delay	800
Outgoing off hook delay	0
On hook delay	300
Type of Call Progress to use for External Calls	How this should be set depends on the gateway used for the integration. <ul style="list-style-type: none">• If the gateway supports call progress through to the endpoint, set to Digital.

- If the gateway reports early that the call is connected, such as before the phone rings or while the phone is ringing, set to **Media**.
-

- 9 Click **Apply** to save the changes.
- 10 To add another failover server repeat **Steps 4-9**.
- 11 Click **OK** to close the **Integration Options** dialog box.

To remove a SIP Failover Server:

- 1 From **MiCollab AM Configuration**, click the **Integrations** tab.
- 2 From the **Integrations** list, select your integration, and then click **Edit**.
- 3 In the **Integration Options** dialog box, go to the **Local Integration Settings** section.
- 4 From the **View** drop-down list, select **Failover Server Settings**.
- 5 In the **Failover Server Settings** view, click the **Remove Failover Server** button.
- 6 At the confirmation prompt, click **Yes** to confirm the deletion.

NOTE If multiple servers are listed, the last server address and port pair on the list is deleted first.

- 7 Click **Apply** to save the changes, and then click **OK** to close the **Integration Options** dialog box.

Configuring Direct-Inward-Dial (DID) Call Routing to MiCollab AM

You can assign a DID that can be called directly from PSTN to MiCollab AM auto attendant. It is recommended that you use the last 4 digits of a designated DID number as the MiCollab AM hunt group access code when configuring endpoint for the new trusted application for MiCollab AM to avoid digit conversion.

If your Skype for Business environment has dial plan configured to normalize numbers to **E.164** format, you must configure a normalization rule for MiCollab AM to keep the hunt group access code in 4-digit and prefix it with a + sign.

NOTES

- MiCollab AM can only support up to a maximum of 10 digits in the **Hunt Group Access Code** field.
- For more information about normalization rules, see: technet.microsoft.com/en-us/library/gg413082.aspx.

You can also configure Skype for Business to automatically route all DID calls directly to MiCollab AM so that DID calls can be processed by MiCollab AM based on how subscriber availability rules are setup.

IMPORTANT In order to route all DID calls to MiCollab AM, you will need to create a normalization rule in the Skype for Business dial plan to translate all subscriber incoming DID numbers to MiCollab AM hunt group access code.

For example:

Assume that **T1 PRI** line is available with 10 DID trunks in the range from **425-555-1200** to **425-555-1209**, and **Telco** switch sends the last four digits in the ISDN set up message.

The goal is to assign the first number to MiCollab AM and the remaining to route directly to MiCollab AM.

PSTN Users Dial	Digits Sent by Telco Switch	Use
425-555-1200	1200	DID line for MiCollab AM
425-555-1201 to 425-555-1209	1201 -1209	DID line for Skype for Business Users

New Copy Paste Select... Show details... Remove			
Normalization rule	State	Pattern to match	Translation pattern
Voicemail 1200	Committed	^(1200)\$	+\$1
4-Digit Extension	Committed	^(120[1-9])\$	+\$1200
7-Digit Local	Committed	^(\d{7})\$	+1425\$1
10-Digit Long Distance	Committed	^(\d{10})\$	+1\$1
International	Committed	^(011\d{7}\d+)\$	+\$1
Keep All	Committed	^(\d+)\$	\$1

Figure 4. Normalization Rules for DID Call Routing

Configuring MiCollab AM to Accept a DID Call Directly on Behalf of a Subscriber

In order for MiCollab AM to accept a DID call directly on behalf of a subscriber, the subscriber must have the following features set up:

- **Availability** enabled

NOTE For more information about **Availability** and how to configure the feature, see the document, *Availability Administration Guide*.

- A list of **Find-me** devices with active **Locate Mode**

IMPORTANT If the **Locate Mode** is configured to go to the primary device and the number for that primary device is the subscriber's Skype for Business number, then you must make sure that the DID number for the subscriber does NOT match their line URI value in Skype for Business.

To avoid this, you can either change the DID number or assign a new phone number for the Skype for Business, and create a new **Extension** as the **Primary Device** with the new number in MiCollab AM for the subscriber.

Retain the original **Primary Device (Extension)** for the subscriber, but it should not be the **Primary Device** and should not be in the **Find-me Devices** list.

For example:

Let's say a subscriber is configured with the following numbers:

- DID: **XXX-XXX-1234**
- Skype for Business: **1234**
- MiCollab AM Extension (Primary Device): **1234**

To differentiate DID and Skype for Business numbers for this subscriber:

1. Change the **Skype for Business** number to **2234**.
2. In MiCollab AM, create a new **Extension** with **2234** and set it as the **Primary Device**.
3. Retain the **Extension** for **1234**, but it will no longer be the **Primary Device**.
4. In the **Find-me Devices** list, make sure the list contains the device with **2234** and NOT **1234**.
5. With this configuration, the DID call will be answered in MiCollab AM as if it's a forwarded call from **1234** and the caller will hear the **Availability** menu.
6. Enable **Auto Locate** for the subscriber or make sure that **Locate** is an option for the caller.
7. MiCollab AM will call the first number on the list at **2234**, which is the subscriber's Skype for Business number.

Enabling Gateway Support

NOTE Gateway support should only be used if your Skype for Business environment does not have direct access to the PSTN or other PBX/Gateways.

This support is only intended to provide access to the PSTN via a PBX integrated to MiCollab AM.

NOTE For information on related integrations, see the appropriate ITN for the PBX integration you are installing.

Critical Application Considerations

Known limitations or conditions within the Skype for Business Server using MiCollab AM as a gateway that affect the performance are listed here. General recommendations are provided as follows to avoid these limitations.

- **911** and **E.911** are not supported via the integration.
- Subscribers must have the appropriate callout permission on MiCollab AM to enable them to place calls to numbers that are not associated with other subscribers via their devices configuration.
- MiCollab AM uses two lines for each call – one to Skype for Business and another one to the PBX.
- Each connection is separate; a security context that may exist on one connection should not be assumed to exist on the joined connection.
- Gateway calls are treated as calls dialed via the answering call processor mailbox. The switch section for this mailbox should not be set to Skype for Business.

Programming the Skype for Business for Gateway Support

In order to obtain gateway support through MiCollab AM server, the following configuration settings should be ensured on the Skype for Business Server:

- A secondary endpoint must be configured for MiCollab AM. All calls received through this secondary endpoint will be considered gateway calls and will be joined with outgoing calls on the secondary integration defined in MiCollab AM.
- A Skype for Business Server application must be created and registered in order to route specific calls to the secondary endpoint for MiCollab AM. This can be a simple **Microsoft SIP Processing Language (MSPL)** script that routes all calls targeting a number with a specific prefix to the secondary endpoint of MiCollab AM.

- One or more normalization rules should be created in order to ensure that calls targeting the gateway will have their target phone number match the pattern required by the routing script. This can be a simple 'catch all' rule with lowest priority that will add the prefix required by the script from the previous step.

Next section presents details for these steps. The example data from this section is provided in the context of the same demonstration environment described at the beginning of the document, with the following additions:

- **1601** = phone number associated with the secondary endpoint for MiCollab AM; the gateway
- **RouteToCXGateway.am** = name of the MSPL script used to route calls to the secondary endpoint of MiCollab AM

Creating Secondary Endpoint

The secondary endpoint will be created using the same command used for creating the primary endpoint, changing only the SIP address and **LineURI** parameters:

```
New-CsTrustedApplicationEndpoint -TrustedApplicationPoolFqdn cx-trusted-apps.sfbdomain.local -ApplicationId cx-voicemail -SipAddress sip:1601@sfbdomain.local -LineURI "tel:+1601" -DisplayName "MiCollab AM Gateway"
```

Table 20. Secondary Endpoint Settings

Argument	Description
TrustedApplicationPoolFqdn	FQDN of the trusted application pool configured for MiCollab AM servers
ApplicationId	Name of the trusted application configured to provide integration between Skype for Business service and MiCollab AM application
SipAddress	SIP address that will be associated to MiCollab AM gateway.
LineURI	Number assigned to MiCollab AM gateway preceded by "tel:+" prefix
DisplayName	Display name associated to this endpoint.

NOTE For more information about these commands, see the [Creating an Endpoint for MiCollab AM](#) section.

Creating and Registering Skype for Business Server Application

Lync Server 2013 SDK provides detailed information about various ways for creating Skype for Business Server applications that can be used for advanced call routing among other purposes.

The simplest approach is to create a MSPL, script only server application. Following is an example of such a script that will route to the endpoint defined above **"sip:1601@sfbdomain.local"** all calls with target phone number starting with **' +12345 '** prefix.

```
<?xml version="1.0"?>
<lc:applicationManifest
  lc:appUri="http://sfbdomain.local/RouteToCXGateway"
  xmlns:lc="http://schemas.microsoft.com/lcs/2006/05">
<lc:requestFilter methodNames="INVITE"
  strictRoute="true"
  registrarGenerated="true"
  domainSupported="true" />
<lc:allowRegistrationBeforeUserServices/>
<lc:responseFilter reasonCodes="NONE" />
<lc:proxyByDefault action="true" />
<lc:scriptOnly />
<lc:splScript><![CDATA[

// The calls to the diagnostics routine Log should be disabled in the release version
// Diagnostics
Log("Debugr", false, Concatenate("RouteToCXGateway: Processing INVITE request with URI= '",
RequestTarget.Uri, "'"));

// Check pre-defined sipRequest object exists. It contains parsed request data
if ( !sipRequest ) {
  // Diagnostics
  Log("Debugr", false, "RouteToCXGateway: ERROR: sipRequest is NULL");
}

// We are interested only in phone calls ... therefore make sure the the request URI is a phone URI
else if ( !RequestTarget.IsPhone ) {
  // Diagnostics
  Log("Debugr", false, "RouteToCXGateway: ERROR: RequestTarget.IsPhone is FALSE");
}

// Make sure the called number starts with the external prefix ... +12345 in this example
else if ( !StartsWithString(GetUserName(RequestTarget.Uri), "+12345", true) ) {
  // Diagnostics
  Log("Debugr", false,
    Concatenate(
      "RouteToCXGateway: WARNING: GetUserName(RequestTarget.Uri)=",
      GetUserName(RequestTarget.Uri),
      "' does not start with 12345. Will not be routed!"));
}

// Finally route call to CX secondary endpoint ... 'sip:1601@sfbdomain.local' in this case
else {
  // Diagnostics
  Log("Debugr", false,
    Concatenate(
      "RouteToCXGateway: DEBUG: GetUserName(RequestTarget.Uri)=",
      GetUserName(RequestTarget.Uri),
      "' starts with 12345. It will be routed!"));

  RetargetRequest("sip:1601@sfbdomain.local");
}

Return;
]]></lc:splScript>
</lc:applicationManifest>
```

In order for the Skype for Business Server to start using this script in its call routing process, the script must be registered with the Skype for Business Server and the Skype for Business Front-End service, **RtcSrv**, must be restarted.

Save the script content provided above to a file called **RouteToCXGateway.am**. For your convenience, place this file in the root folder of Skype for Business Server installation, usually:

C:\Program Files\Skype for Business Server\Server\Core

NOTE Changing the name or the location of this file will require appropriate changes to the parameters passed to registration command presented below.

The following PowerShell command must be used in order to register the script with Skype for Business:

```
New-CsServerApplication -Uri "http://sfbdomain.local/RouteToCXGateway" -Identity
"Service:Registrar:SFB.sfbdomain.local/RouteToCXGateway" -Critical $False -Priority 1
-Scriptname RouteToCXGateway.am -Enabled $True
```

Table 21. Skype for Business Server Settings

Argument	Description
Uri	Unique Uniform Resource Identifier (URI) for the application. This value must match the attribute " lc:appUri " defined in the script.
Identity	Unique identifier for the server application. This value must match the following pattern: "Service:Registrar:" + FQDN for Skype for Business registrar (usually the Front End server) + "/" + <unique name>
Critical	This should be set to \$False so that the Skype for Business Server should be able to start even in the unlikely case this application fails to initialize and start.
Priority	A value that will determine the order in which registered Skype for Business Server application are executed. Smaller numbers indicate a higher priority.
Scriptname	Path to the script file. Relative paths are considered relative to the <i>Core</i> folder of the Skype for Business Server installation.
Enabled	Set this to \$True in order for the Skype for Business Server to use the application.

NOTES

1. For more information about this command see: technet.microsoft.com/en-us/library/gg398096.aspx
2. The **RtcSrv** service on the Skype for Business Front End server must be restarted in order for Skype for Business to start using the new application

It is recommended to test the script before registering it, in order to make sure there are no syntax errors. This is especially necessary when the content of the script is modified.

The validity of the syntax is verified with the **CompileSPL.exe** tool from the Lync Server 2013 SDK. After installing the Lync 2013 Server SDK in the default location, the tool can be used from a command prompt and expects as parameter the file path for the script to the test:

C:\Program Files\Lync Server 2013\sdk\bin\compilespl.exe

C:\Program Files\Skype for Business Server\server\core\routetocxgateway.am

NOTE For more information about Lync Server 2013 SDK, and creating and registering the Skype for Business Server application, review the information from Microsoft website:
[msdn.microsoft.com/en-us/library/office/dn454964\(v=office.15\).aspx](https://msdn.microsoft.com/en-us/library/office/dn454964(v=office.15).aspx).

Creating Normalization Rule to Add the Routing Prefix

This step consists in creating a normalization rule in the dial plan that will add the prefix required by the routing script to the numbers to be dialed through the gateway.

Configuring MiCollab AM for Gateway

- Review the [Critical Application Considerations](#) section.
- Enable the gateway option in the integration see the [Configuring MiCollab AM](#) section.

Changing the Network Binding Order on the MiCollab AM Platform

If your MiCollab AM server platform is a component of two or more local or wide area networks (LANs or WANs), you must make sure that this integration does not interfere with the normal network operation of the server. By default, MiCollab AM uses the primary (public) network interface card (NIC) in the platform, the first NIC in the network binding order. If you want MiCollab AM to use a NIC other than the first one, you must make several required configuration changes. It is much easier to configure the Integration to use another NIC by simply setting the integration parameter **Local IP Address to bind on** to the address of the NIC connected to the PBX.

NOTE The operating system gives precedence to the first network connection in the list followed by the remaining connections based on their position in the list.

The instructions in this section ensure that the binding order is correct when you set up the integration. If you replace a NIC on the MiCollab AM server platform later, the platform's operating system registers the new adapter at the bottom of its binding order. Restoring the original binding order should correct any problems caused by the change.

IMPORTANT The following procedure shifts the binding order of the network interface cards. To determine which NIC is associated with a specific network connection, right-click the connection in the **Network Connections** window, and then select **Properties**.

Windows Server 2012 R2

To change the binding order of multiple NICs:

- 1 From the taskbar, click **Start > Control Panel**.
- 2 In the **Control Panel**, click **Network and Internet > Network and Sharing Center**.
- 3 On the left pane, select **Change Adapter Settings**.
- 4 Press **Alt** to display the menu bar.
- 5 On the menu bar, select **Advanced**, and then click **Advanced Settings**.
- 6 On the **Adapters and Bindings** tab of **Advanced Settings**, click the network connection that serves MiCollab AM.
- 7 Click the up arrow button to the right of the **Connections** list as many times as needed to move the connection to the top of the list.
- 8 Click **OK**, and then close the **Network Connections** window and the **Control Panel**.

Windows Server 2016 / 2019

To change the binding order of multiple NICs:

- 1 From the taskbar, select **Start > Control Panel**.
- 2 In the **Control Panel**, click **Network and Internet > Network and Sharing Center**.
- 3 On the left pane, select **Change Adapter Settings**.
- 4 Right-click the network connection that serves MiCollab AM and then select **Properties**.
- 5 On the **Networking** tab of the **Local Area Connection Properties** dialog box, select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
- 6 On the **General** tab of the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, click the **Advanced** button.
- 7 On the **IP Settings** tab of the **Advanced TCP/IP Settings** dialog box, clear the **Automatic metric** check box and then type in a low value in the **Interface metric** field. The lower the value, the higher the priority.

NOTE For all Windows systems, the value 1 is reserved for the loopback adapter. It is recommended to use a value of 2 or higher for the network connection that serves MiCollab AM.

- 8 Click **OK** on all of the dialog boxes to save the settings, and then close the **Local Area Connection Properties** dialog box.
- 9 Repeat steps 4 through 8 to assign an Interface metric value to all other network adapters.

Configuring Quality of Service (QoS)

As of version 6.0, MiCollab AM has no internal support for QoS. QoS must now be implemented externally via group policies as Policy-Based QoS. See your operating system's documentation for details.

Table 22. QoS Configuration

Field	Setting
Application Name	At_TelephonyServer.exe
Protocol	Match the setting used for the integration UDP or TCP
Source Port	<p>MiCollab AM requires a range of ports for audio support. The MiCollab AM audio ports start at the Local Media Base UDP Port configured in the Server tab. Each MiCollab AM line reserves 10 ports. Hence, the port range starts from the number configured there, and goes to the last port of the last line. The formula for calculating the highest port number in the range is as follows:</p> $\text{BasePortNumber} + (\text{NumberOfCXPorts} * 10) - 1.$ <p>Hence, if the base port is 10000, and MiCollab AM has 8 lines, then the port range to use would be:</p> <p>10000:10079</p>
DSCP Value	46

Appendix A – Converting Trusted Application Pool Certificate from PFX Format to PEM

Download **OpenSSL** binaries and execute the following commands:

- To generate key file:

```
openssl.exe pkcs12 -nodes -nocerts -in cx-trusted-apps.pfx -out cx-trusted-apps.key.pem
```

- To generate certificate file:

```
openssl.exe pkcs12 -nokeys -in cx-trusted-apps.pfx -out cx-trusted-apps.cer.pem
```

NOTE You can download **OpenSSL** binaries from openssl.org.

cx-trusted-apps.pfx file specified as value for the **in** argument in the commands above is the exported certificate for the trusted application pool.

The examples above assume that the **cx-trusted-apps.pfx** file is located in the same folder as the **openssl** executable.

Appendix B – Configuring MiCollab AM to Use Certificate Files Directly

If you cannot use the certificates from the Windows certificates store for any reason, then you can configure MiCollab AM to use the certificate files directly by clearing the **Thumbprint call server certificate** and **Thumbprint remote root CA certificate** properties from the **Connection Security Settings** integration settings.

IMPORTANT Although you can configure MiCollab AM to use the certificate files directly, this method is not recommended as it is less secure.

In order to perform the tasks, follow **Steps 1** through **9** from the [Configuring MiCollab AM](#) section, replace **Step 10** with the instructions explained below, and continue on to **Step 11**.

To use certificate files directly on MiCollab AM:


These steps replace **Step 10** from the [Configuring MiCollab AM](#) section.


- 1 Select **Connection Security Settings** from the **View** drop-down list.
- 2 Unselect the **Show Thumbprint properties [allow selection of certificates from Windows certificate store]** checkbox. The editor displays the **Local Certificate FileName** and **Local Private Key FileName** options.

The screenshot shows the 'Integration Options' dialog box. The 'Local Integration Settings' section is expanded, showing a table of settings. The 'View' dropdown is set to 'Connection Security Settings'. The 'Local Certificate FileName' and 'Local Private Key FileName' fields are highlighted with a red box. The 'Show thumbprint properties [allow selection of certificates from Windows certificate store]' checkbox is also highlighted with a red box.

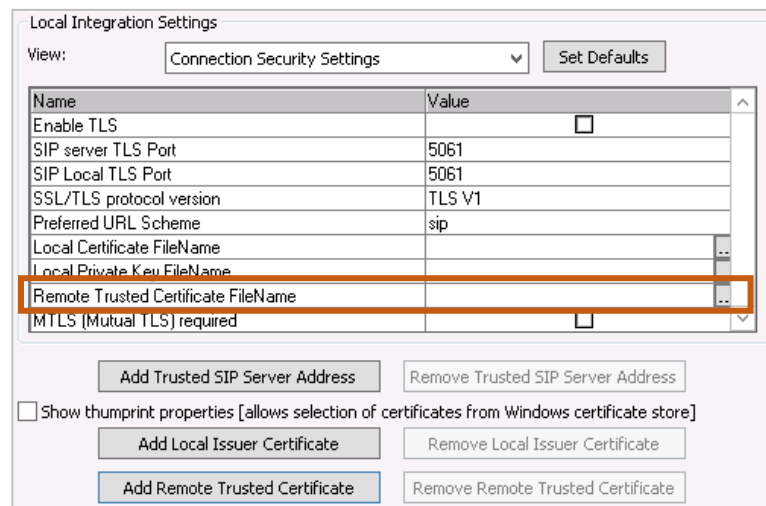
Name	Value
SIP Server Address	SFB2015.sfbdomain.local
SIP Server Address	SFB-FE1.sfbdomain.local
SIP server TLS Port	5061
SIP Local TLS Port	5061
SSL/TLS protocol version	TLS V1
Preferred URI Scheme	sip
Local Certificate FileName	... \cx-trusted-apps_6d3b91a4-9b9e-4...
Local Private Key FileName	... \cx-trusted-apps_6d3b91a4-9b9e-4...
Remote Trusted Certificate FileName	...

☐ Show thumbprint properties [allow selection of certificates from Windows certificate store]

- 3 From the **Local Certificate FileName** and **Local Private Key FileName** *Value* columns, click the  to locate the PFX file that contains the certificate and the private key for the trusted application.
- 4 Once you select the file for each option, the MiCollab AM configuration application will automatically export the certificate and the private key in PEM format in new files under the Certificates folder in the MiCollab AM installation.
- 5 If successfully exported, the **Local Certificate FileName** and **Local Private Key FileName** *Value* fields are filled with the path to the appropriate file.

NOTE If the certificate and its private key are already available in the PEM format, then use the  browse button of the appropriate property to set that file to be used by MiCollab AM.


- 6 In order to configure the certificate to be used by MiCollab AM for the root CA in the certification path of the Skype for Business certificate, click the **Add Remote Trusted Certificate**. This will add a new entry called **Remote Trusted Certificate FileName**.



Name	Value
Enable TLS	<input type="checkbox"/>
SIP server TLS Port	5061
SIP Local TLS Port	5061
SSL/TLS protocol version	TLS V1
Preferred URL Scheme	sip
Local Certificate FileName	..
Local Private Key FileName	..
Remote Trusted Certificate FileName	..
MTLS (Mutual TLS) required	<input type="checkbox"/>

Buttons: Add Trusted SIP Server Address, Remove Trusted SIP Server Address, Add Local Issuer Certificate, Remove Local Issuer Certificate, **Add Remote Trusted Certificate**, Remove Remote Trusted Certificate.

☐ Show thumbprint properties [allows selection of certificates from Windows certificate store]

- 7 Use the  browse button to select the certificate for root CA in the certification path of the Skype for Business certificate.

NOTE Make sure that the certificate is in the PEM format.

In order to check its format, open the file using notepad. If the file is in binary format, notepad will display characters that are not part of the printable ASCII range. Then, it needs to be converted to the PEM format.

To convert it the certificate:

- a Right-click on the file, and select **Open** from the contextual menu.
- b The new **Certificate** dialog appears. Select the **Details** tab.
- c In the **Details** tab, click the **Copy to File** button. The Windows certificate export wizard appears.
- d During the export, select the **Base-64 encoded X.509 (.CER)** option.
- e Use the converted file to continue configuring MiCollab AM.