

MiCollab Advanced Messaging Cisco Unified Communications Manager 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	4
References	4
Documentation	4
Documentation Updates	5
Help	5
Document Conventions	5
Features Supported by This Integration	6
Critical Application Considerations	9
Installation Requirements	11
Telephone System Requirements	11
MiCollab AM Requirements	11
Programming the Telephone System	12
Configure the SIP Trunk Security Profile	12
Configure the SIP Profile	13
Configure Common Device Configuration	14
Configure the SIP Trunk	16
Route Group Configuration	20
Route List Configuration	21
Verifying Route List Configuration	22
Configuring Route Pattern	23
Resetting SIP Trunk	23
Configuring MiCollab AM	25
Configuring MiCollab AM for the Integration During Initial Installation	25
Configuring Existing MiCollab AM for the Integration	28
Configuring MiCollab AM for SIP Failover	32
Configuring MiCollab AM for TLS and SRTP	34
Changing the Network Binding Order on the MiCollab AM Platform	39
Windows Server 2012 R2	39
Windows Server 2016 / 2019	40
Configuring Quality of Service (QoS)	41

Preface

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 Cisco Unified Communications Manager (CallManager) and SIP.

This document describes how to integrate MiCollab AM with a Cisco Unified Communications Manager system using SIP. Critical application considerations are documented, as well as installation and programming procedures necessary to integrate MiCollab AM with Cisco Unified Communications Manager, referred to throughout this document as Unified CM.

The Unified Communications Manager is the software-based call-processing component of the Cisco IP telephony solution. SIP is a call control signaling protocol used by Unified CM to set up calls between the Unified CM server and other devices, such as IP telephones and MiCollab AM. SIP is used for registration of handsets and gateways with Unified CM, and for call processing functions such as call setup, teardown, and supplementary services.

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 Unified CM and SIP, please refer to the appropriate Cisco documentation.

Features Supported by This Integration

The following tables list the features supported using the Cisco Unified Communications Manager SIP integration.

Table 2. Call forward to personal greeting support for these common call types

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

Table 3. Integration features supported for Cisco Unified Communications Manager SIP

Feature	Supported	Notes
Automatic subscriber logon	Yes	
ANI/CLI	Yes	
Announce Busy greeting on forward busy calls	Yes	
Call screening	Yes	
Caller queuing	Yes	Note 1
DNIS	No	
End-to-end DTMF, attendant console	Yes	
End-to-end DTMF, proprietary telephones	Yes	
Fax Tone Detection	Yes	
Internal calling party ID for reply	Yes	
IPv6	Yes	
Live record, integrated	No	
Live reply to sender	Yes	
Message notification callouts	Yes	Note 2
MWI, set/clear	Yes	
MWI, inband/outband	Inband	
Networking, analog	Yes	
Overflow from MiCollab AM to attendant	Yes	
Overflow to MiCollab AM from attendant	Yes	
PBX-provided disconnect signaling	Yes	
Revert to operator	Yes	
SRTP	Yes	
TLS	Yes	

Transfers, blind	Yes	Note 3
Transfers, confirmed	Yes	
Transfers, fully supervised	Yes	
Transfers, monitored	Yes	
Trunk ID for call routing	No	
Multiple Integrations	Yes	Note 4

NOTES

1. Caller Queuing is specific to each local Call Server. Call Servers within the system are unaware of queued calls to the same subscriber on other Call Servers. For more information, refer to the note in the next section, [Critical Application Considerations](#).
2. Do not direct message notification callouts to a station that is forwarded to MiCollab AM.
3. See the note regarding blind transfers in the next section, [Critical Application Considerations](#).
4. See [Critical Application Considerations](#).

Critical Application Considerations

Known limitations or conditions within the telephone system and MiCollab AM that affect the integration performance are listed here. General recommendations are provided when ways to avoid these limitations exist.

- On a MiCollab AM server with two or more NICs, the NIC that supports this integration must not occupy first place in the operating system's binding order. The primary (public) network interface card (NIC) must be the first network connection in the network binding order. MiCollab AM binds and communicates to other servers and subscribers on this network connection. For more information, refer to [Changing the Network Binding Order on the MiCollab AM Platform](#).
- MiCollab AM supports G.729a with support for annex b on the incoming audio stream only. MiCollab AM does not transmit annex b packets.
- When codec negotiation takes place between MiCollab AM and the PBX, MiCollab AM always offers the G.729a audio format as an option. You may configure G.729a as the preferred codec in MiCollab AM; however, the decision whether to use G.729a is always made by the PBX.
- The Call Queuing feature does not transcend the Call Server. Calls may be queued on multiple Call Servers for the same subscriber but Call Servers do not have knowledge of calls in the queue on other Call Servers within the system. Callers may be prompted with specific information about their place in the queue; however, the information pertains to the specific Call Server on which their call is queued.
- Before it initiates a blind transfer, Cisco Unified Communications Manager evaluates the destination number against its dial plan. If the destination number satisfies the criteria in the dial plan, Unified CM then initiates the transfer using the same method as it would if a subscriber pressed a transfer key on one of the system's extension telephones. Because of this, a blind transfer to a destination number that does not satisfy the dial plan criteria may fail. Note also that in such cases, Unified CM may hold the line active until it finally drops the caller. If Unified CM has failed over to a Survivable Remote Site Telephony (SRST) router, such transfers cause MiCollab AM line ports to become out of service.
- Do not use the MiCollab AM immediate message notification feature with any station programmed to forward to voice mail. If MiCollab AM attempts an immediate message notification callout to a station programmed to forward to MiCollab AM, and that station is busy or ring-no-answer (RNA), the callout forwards to the subscriber's mailbox.
- Non-numeric DTMF tones cannot be used as any character in the station number. The maximum length of a station number is ten digits.
- Unified CM performs its own call progress detection, and MiCollab AM relies on that call progress detection for all calls that it receives through Unified CM. This configuration may provide call progress detection results that vary slightly from the results obtained through integration with a circuit-switched telephone system. If subscribers encounter silence or ring tones that seem confusing, contact the Cisco Technical Assistance Center (TAC), either by telephone or at www.cisco.com, for information on how to adjust Unified CM call progress detection.

- Do not activate the operating system's Network Teaming driver to allow teamed network interface cards (NICs). This feature can interfere with the integration.
- Depending on the characteristics of the network, you may need to adjust the size of the memory buffer that the system provides to protect against jitter distortion in the voice signals it processes. Use the **mgcp playout** command to adjust this parameter on Cisco routers. In some cases, an initial buffered play-out value of 200 ms and an upper limit of 250 ms (as set by the command **mgcp playout adaptive 200 4 250**) works well; however, you may need to adjust these values for the characteristics of your network.
- If the telephone system is configured to fail over to a Cisco router with SRST capabilities, MWI operations become inoperable until service is restored on the telephone system. In addition, because the number of priority levels that can be assigned to lines in a hunt group is limited to ten on the router, only ten lines can be active during failover.
- On the **Hunt Pilot Configuration** page, be sure that the **Connected Line ID Presentation** field is set to **Default** or **Allowed**. A setting of **Restricted** causes calls to the hunt pilot number to answer non-integrated.
- 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 Avaya Communication Manager 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 integration successfully, you must meet the installation requirements for both the telephone system and MiCollab AM.

Telephone System Requirements

Please refer to the Cisco website, www.cisco.com, for a complete list of current part numbers for the following products:

- Cisco Media Convergence Server (MCS) or other Cisco approved server
- Cisco Unified Communications Manager version 12.5 or prior supported versions
- Cisco SRST router with IOS software version 15.1 or prior supported versions

MiCollab AM Requirements

- MiCollab AM software version 9.1
- MiCollab AM software key diskette or feature file with Cisco Unified Communications Manager SIP Integration enabled and one Virtual SIP and RTP license enabled for each Cisco port involved in the integration
- One or two 10 MB, 100 MB, or 1000 MB (gigabit) network interface cards with cables

Programming the Telephone System

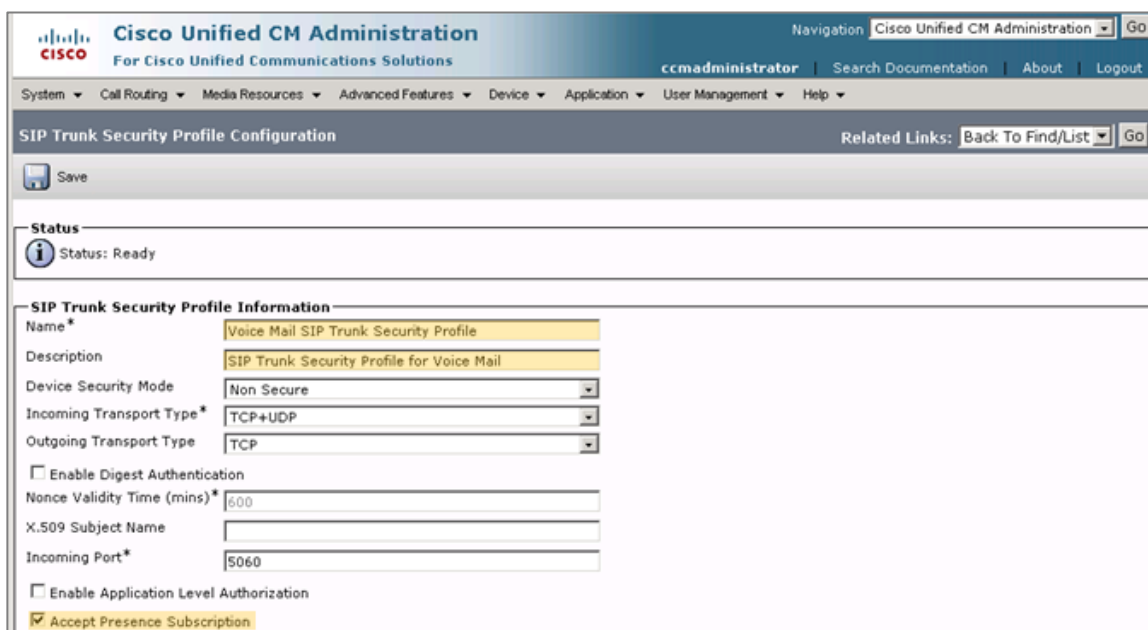
To configure the Cisco Unified Communications Manager for Direct SIP integration, you must perform the following steps in the following order:

- Configure the SIP trunk security profile
- Configure the SIP profile
- Configure the Common Device Configuration
- Configure the SIP trunk
- Configure the route group
- Configure the route list
- Configure the route pattern.

Configure the SIP Trunk Security Profile

To configure the SIP trunk security profile:

- 1 Navigate to **System > Security > SIP Trunk Security Profile**.
- 2 Click **Add New** on the screen that appears. The **SIP Trunk Security Profile Configuration** appears.
- 3 Enter a **Name** and **Description** for the SIP trunk security profile.
- 4 Select the **Accept Presence Subscription**, **Accept Unsolicited Notification**, and **Accept Replaces Header** checkboxes.

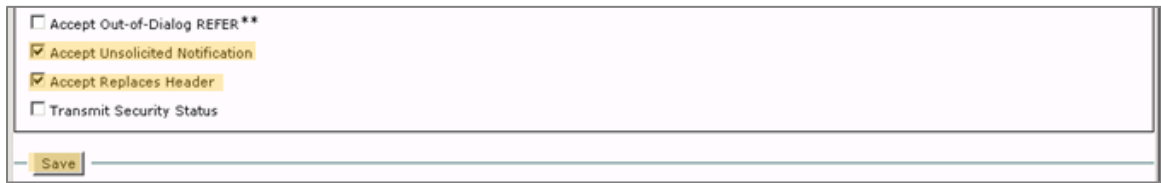


The screenshot displays the Cisco Unified CM Administration web interface. The top navigation bar includes the Cisco logo, the title "Cisco Unified CM Administration", and a navigation menu with options like "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", and "Help". The main content area is titled "SIP Trunk Security Profile Configuration" and includes a "Save" button. Below this, there is a "Status" section showing "Status: Ready". The "SIP Trunk Security Profile Information" section contains the following fields and options:

- Name***: Voice Mail SIP Trunk Security Profile
- Description**: SIP Trunk Security Profile for Voice Mail
- Device Security Mode**: Non Secure (dropdown)
- Incoming Transport Type***: TCP+UDP (dropdown)
- Outgoing Transport Type**: TCP (dropdown)
- ☐ Enable Digest Authentication
- Nonce Validity Time (mins)***: 600
- X.509 Subject Name**: (empty field)
- Incoming Port***: 5060
- ☐ Enable Application Level Authorization
- ☒ Accept Presence Subscription

Image continued on next page

Image continued from previous page



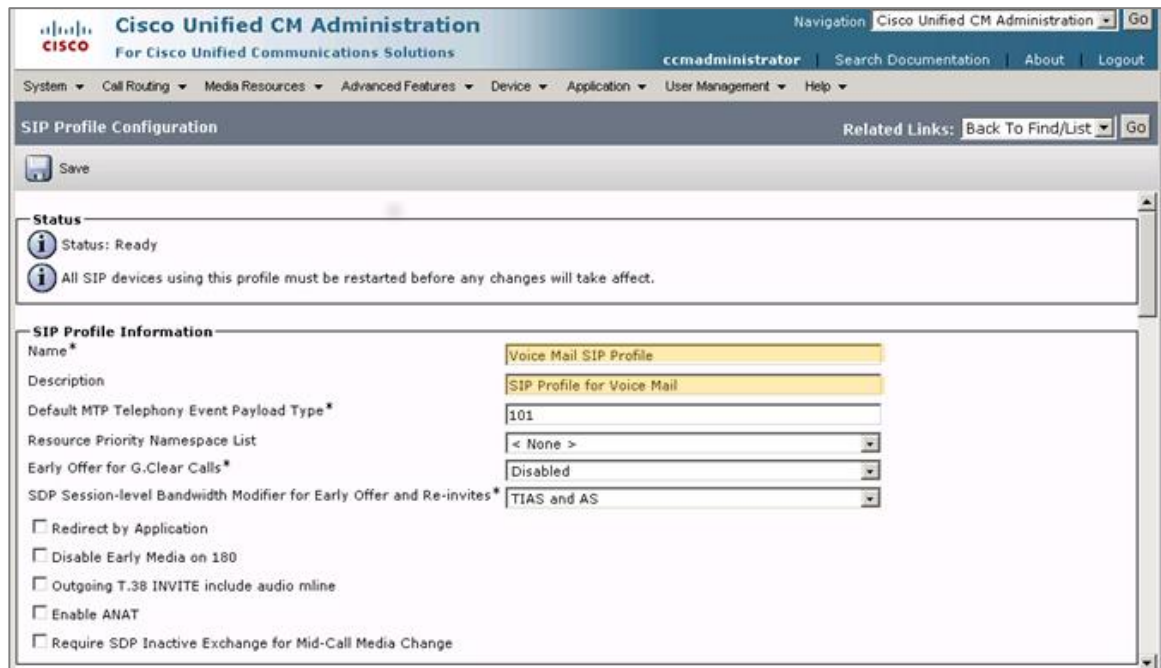
A screenshot of a web form for SIP profile configuration. It contains four checkboxes: 'Accept Out-of-Dialog REFER **' (unchecked), 'Accept Unsolicited Notification' (checked), 'Accept Replaces Header' (checked), and 'Transmit Security Status' (unchecked). A 'Save' button is located at the bottom left of the form.

- 5 Click **Save**.

Configure the SIP Profile

To configure the SIP profile:

- 1 Navigate to **Device > Device Settings > SIP Profile**.
- 2 Click **Add New** on the screen that appears. The **SIP Profile Configuration** screen appears.



A screenshot of the 'SIP Profile Configuration' screen in the Cisco Unified CM Administration interface. The page title is 'Cisco Unified CM Administration For Cisco Unified Communications Solutions'. The user is logged in as 'ccmadministrator'. The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, and Help. The 'SIP Profile Configuration' section is active, showing a 'Save' button and a 'Status' section with 'Status: Ready' and a message: 'All SIP devices using this profile must be restarted before any changes will take effect.' The 'SIP Profile Information' section contains the following fields: 'Name' (Voice Mail SIP Profile), 'Description' (SIP Profile for Voice Mail), 'Default MTP Telephony Event Payload Type' (101), 'Resource Priority Namespace List' (< None >), 'Early Offer for G.Clear Calls' (Disabled), and 'SDP Session-level Bandwidth Modifier for Early Offer and Re-invites' (TIAS and AS). There are also several unchecked checkboxes: 'Redirect by Application', 'Disable Early Media on 180', 'Outgoing T.38 INVITE include audio mline', 'Enable ANAT', and 'Require SDP Inactive Exchange for Mid-Call Media Change'.

- 3 Enter a **Name** and **Description** for the SIP Profile.
- 4 Scroll further down the screen and check the **Enable VAD** field.



A screenshot of the 'SIP Profile Configuration' screen, showing the 'Parameters used in Phone' section. The parameters are: 'Timer Invite Expires (seconds)' (180), 'Timer Register Delta (seconds)' (5), and 'Timer Register Expires (seconds)' (3600). The 'Save' button is visible at the top left of the form.

Image continued on next page

Image continued from previous page

Timer T1 (msec)*	500
Timer T2 (msec)*	4000
Retry INVITE*	6
Retry Non-INVITE*	10
Start Media Port*	16384
Stop Media Port*	32766
Call Pickup URI*	x-cisco-serviceuri-pickup
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup
Call Pickup Group URI*	x-cisco-serviceuri-gpickup
Meet Me Service URI*	x-cisco-serviceuri-meetme
User Info*	None
DTMF DB Level*	Nominal
Call Hold Ring Back*	Off
Anonymous Call Block*	Off
Caller ID Blocking*	Off
Do Not Disturb Control*	User
Telnet Level for 7940 and 7960*	Disabled
Timer Keep Alive Expires (seconds)*	120
Timer Subscribe Expires (seconds)*	120
Timer Subscribe Delta (seconds)*	5
Maximum Redirections*	70
Off Hook To First Digit Timer (milliseconds)*	15000
Call Forward URI*	x-cisco-serviceuri-cfwdall
Speed Dial (Abbreviated Dial) URI*	x-cisco-serviceuri-abbrdial
<input checked="" type="checkbox"/> Conference Join Enabled	
<input type="checkbox"/> RFC 2543 Hold	
<input checked="" type="checkbox"/> Semi Attended Transfer	
<input checked="" type="checkbox"/> Enable VAD	
<input type="checkbox"/> Stutter Message Waiting	

- 5 Scroll to the bottom of the screen and click **Save**.

Configure Common Device Configuration

To configure a common device:

- 1 Navigate to **Device > Device Settings > Common Device Configuration**.
- 2 Click **Add New** on the screen that appears. The **Common Device Configuration** screen appears.

The screenshot shows the Cisco Unified CM Administration web interface. The top navigation bar includes the Cisco logo, the title "Cisco Unified CM Administration", and a "Go" button. Below the navigation bar, there is a breadcrumb trail: "System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Administration > Help". The main content area is titled "Common Device Configuration". It includes a "Related Links" section with a "Back To Find/List" link and a "Go" button. Below this, there is a "Status" section showing "Status: Ready". The "Common Device Configuration Information" section displays the configuration for "MigratedCommonDeviceConfig1 (942 members**)". The configuration details include: Name (MigratedCommonDeviceConfig1), Softkey Template (Standard User), User Hold MOH Audio Source (1-SampleAudioSource), Network Hold MOH Audio Source (1-SampleAudioSource), and User Locale (< None >).

Image continued on next page

IP Addressing Mode*	IPv4 and IPv6
IP Addressing Mode Preference for Signaling*	IPv6
<input type="checkbox"/> Use Trusted Relay Point	
Use Intercompany Media Services (IMS) for Outbound Calls*	Default

IPv6 for Phones

Allow Auto-Configuration for Phones*	Default
Allow Duplicate Address Detection*	Default
Accept Redirect Messages*	Default
Reply Multicast Echo Request*	Default

MLPP and Confidential Access Level Information

MLPP Indication*	Default
MLPP Preemption*	Default
MLPP Domain	< None >
Confidential Access Mode	< None >
Confidential Access Level	< None >

Save Delete Copy Reset Apply Config Add New

3 Enter a Name for the Common Device Configuration.

4 In the IP Addressing Mode field, choose the version of IP address that the device (SIP trunk or phone that runs SCCP) uses to connect to unified CM.

- **IPv4 Only** – The device uses an IPv4 address to connect to unified CM for both media and signaling events.
- **IPv6 Only** – The device uses an IPv6 address to connect to unified CM for both media and signaling events.
- **IPv4 and IPv6** – The dual-stack device uses either and IPv4 or an IPv6 to connect to the unified CM for both media and signaling events. If only an IPv4 or IPv6 is available for a device (not both types of IP addresses), the device uses the available IP address to negotiate the call.

If the device has both IP address types for both signaling and media events, Cisco Unified Communications Manager uses the configuration for IP Addressing Mode Preference for Signaling setting for signaling events and the IP Addressing Mode Preference for Media enterprise parameter for media events.

5 In the IP Addressing Mode Preference for Signaling, choose the version of IP address that the phone prefers to establish a connection to unified CM during a signaling event for dual-stack devices.

- **IPv4** – The dual-stack device prefers to establish a connection via an IPv4 address during a signaling event.
- **IPv6** – The dual-stack device prefers to establish a connection via an IPv6 address during a signaling event.
- **Use System Default** – The configuration for the enterprise parameter, IP Addressing Mode Preference for Signaling, applies

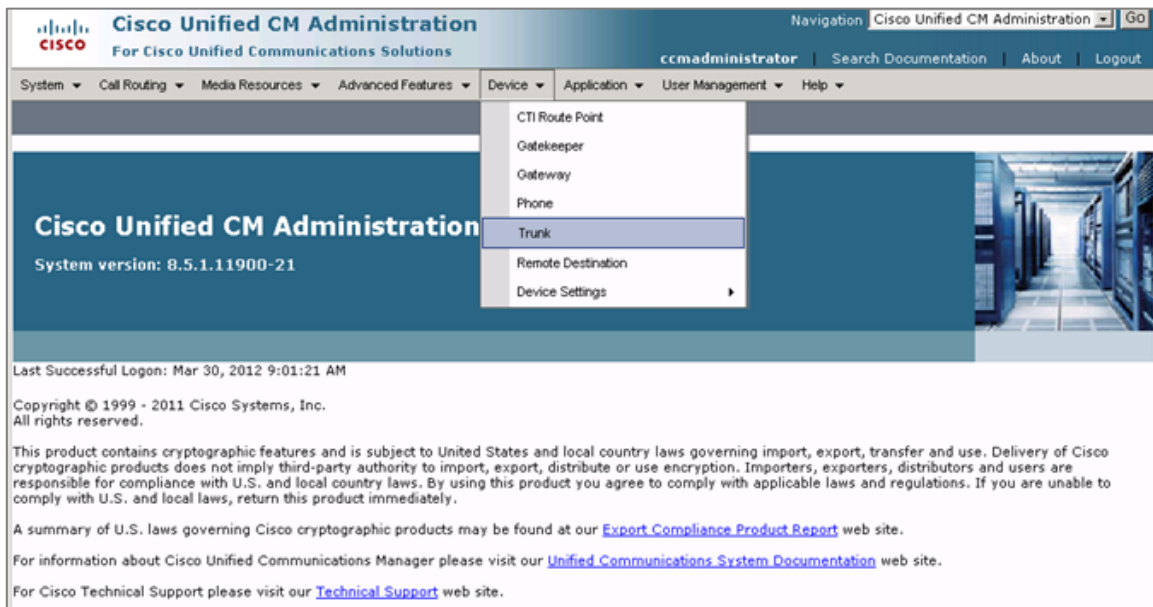
NOTE To enable IPv6 for the Cisco Unified Communications Manager, you must first enable IPv6 on the cluster in Cisco Unified Communications Operating System follow by configuring the unified CM at the application level for device (SIP trunk and phone) and intra-cluster communications. Please refer to the Cisco website, www.cisco.com, for more details on how to enable IPv6 for unified CM.

Configure the SIP Trunk

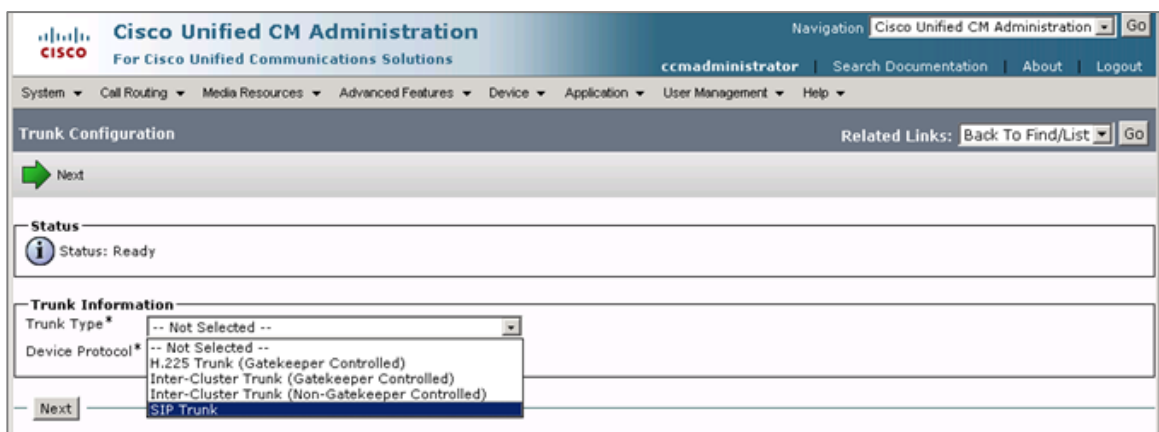
NOTE In systems running more than one call server, a SIP Trunk must be created for each call server in the system that will be running the Cisco Unified Communications Manager SIP Trunk integration. If multiple call servers are to be managed with a SIP router, then a SIP trunk must be created for the SIP router as well.

To configure the SIP Trunk:

- 1 Navigate to **Device > Trunk**.



- 2 Click **Add New** on the screen that appears.



- 3 In the **Trunk Type**, select **SIP Trunk** and click **Next**.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

ccmadministrator Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Help

Trunk Configuration Related Links: Back To Find/List Go

Next

Status
Status: Ready

Trunk Information
 Trunk Type* SIP Trunk
 Device Protocol* SIP
 Trunk Service Type* None(Default)

Next

4 On the screen appears, configure the following options:

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

ccmadministrator Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Help

Trunk Configuration Related Links: Back To Find/List Go

Save

Status
Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	Voice_Mail_SIP_Trunk
Description	SIP Trunk for Voice Mail
Device Pool*	Default
Common Device Configuration	MigratedCommonDeviceConfig1
Call Classification*	OnNet
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0

☐ Media Termination Point Required
☒ Retry Video Call as Audio
☐ Path Replacement Support
☐ Transmit UTF-8 for Calling Party Name
☐ Transmit UTF-8 Names in QSIG APDU
☐ Unattended Port
☒ **SRTP Allowed** - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
 Consider Traffic on This Trunk Secure* When using sRTP Only
 Route Class Signaling Enabled* Default
 Use Trusted Relay Point* Default
☒ PSTN Access
☐ Run On All Active Unified CM Nodes

Intercompany Media Engine (IME)
E.164 Transformation Profile < None >

Multilevel Precedence and Preemption (MLPP) Information
MLPP Domain < None >

- a Enter a name in the **Device Name** field. This name must not contain spaces.
 - b Enter a description in the **Description** field.
 - c Select **Default** for **Device Pool**.
 - d Select the **Common Device Configuration** name created previously in the [Configure Common Device Configuration](#) section.
 - e Select **OnNet** for **Call Classification**.
 - f Check the **SRTP Allowed** box if **Consider Traffic on This Trunk Secure** should be selected as **When using sRTP Only**.
- 5 Scroll down to the **Call Routing Information** section, and configure the following options.

The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes the Cisco logo, the title 'Cisco Unified CM Administration', and a navigation menu. The main content area is titled 'Trunk Configuration' and contains a 'Save' button. The 'Call Routing Information' section is expanded, showing the following settings:

- Remote-Party-Id:**
 - ☐ Remote-Party-Id
 - ☒ Asserted-Identity
 - Asserted-Type*: PAI
 - SIP Privacy*: None
- Inbound Calls:**
 - Significant Digits*: All
 - Connected Line ID Presentation*: Default
 - Connected Name Presentation*: Default
 - Calling Search Space: SIP_CSS
 - AAR Calling Search Space: < None >
 - Prefix DN:
 - ☒ Redirecting Diversion Header Delivery - Inbound
- Incoming Calling Party Settings:**

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Buttons: Clear Prefix Settings, Default Prefix Settings

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default		< None >	<input checked="" type="checkbox"/>
- Connected Party Settings:**
 - Connected Party Transformation CSS: < None >
 - ☒ Use Device Pool Connected Party Transformation CSS
- Outbound Calls:**
 - Called Party Transformation CSS: < None >
 - ☒ Use Device Pool Called Party Transformation CSS
 - Calling Party Transformation CSS: < None >
 - ☒ Use Device Pool Calling Party Transformation CSS
 - Calling Party Selection*: Originator
 - Calling Line ID Presentation*: Default
 - Calling Name Presentation*: Default
 - Caller ID DN:
 - Caller Name:
 - ☒ Redirecting Diversion Header Delivery - Outbound

- a Deselect the **Remote-Party-Id** box.
- b Select **PAI** in the **Asserted-Type** field.
- c Select **None** in the **SIP Privacy** field.

- d Check the box for the following two fields:
- **Redirecting Diversion Header Delivery – Inbound**
 - **Redirecting Diversion Header Delivery – Outbound**

6 Scroll down to the **Call Routing Information** section, and configure the following options.

- a In **Destination Address**, enter the IPv4/IPv6 IP address of the MiCollab AM Voice Mail call server that is handling this SIP trunk.

NOTE If a SIP router is being deployed and this is the trunk designated for the SIP router, then this should be the IP address of the server that will run the SIP router.

- b In **SIP Trunk Security Profile**, select the security profile in the previous [Configure the SIP Trunk Security Profile](#) section. All trunks created for multiple call servers and the SIP router can share the same SIP Trunk Security Profile.
- c In **SIP Profile**, select the SIP profile created in the previous [Configure the SIP Profile](#) section. All trunks created for the multiple call servers and SIP router can share the same SIP Profile.

7 Click **Save**.

8 To add more trunks, in **Related Links** located at the upper-right corner of the window, select **Back to Find/List** and then click **Go**.

Route Group Configuration

To Configure the Route Group:

- 1 Navigate to **Call Routing > Route/Hunt > Route Group**.
- 2 Click **Add New** on the screen that appears. The **Route Group Configuration** screen appears.
- 3 In the **Route Group Configuration** screen, configure the following options:

The screenshot shows the 'Route Group Configuration' page in the Cisco Unified CM Administration interface. The page has a blue header with the Cisco logo and navigation links. Below the header is a breadcrumb trail: System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Help. The main content area is titled 'Route Group Configuration' and includes a 'Save' button. The configuration is organized into several sections: 'Status' (Status: Ready), 'Route Group Information' (Route Group Name: Voice Mail SIP Route Group, Distribution Algorithm: Circular), 'Route Group Member Information' (Find Devices to Add to Route Group: Device Name contains, Available Devices list with 'Voice Mail SIP Trunk' selected, Port(s): None Available, Add to Route Group button), and 'Current Route Group Members' (Selected Devices (ordered by priority): Voice Mail SIP Trunk (All Ports), Removed Devices: empty list, Reverse Order of Selected Devices button). A 'Save' button is at the bottom left.

- a Enter a name in the **Route Group Name** field.
- b Look through the **Available Devices** list, and select the Sip Trunk created in the previous [Configure the SIP Trunk](#) section, and then click **Add To Route Group**.

NOTE If a SIP Router is being deployed, then the trunk selected should be the one designated for the SIP router.

- 4 Click **Save**.

Route List Configuration

To Configure the Route List:

- 1 Navigate to **Call Routing > Hunt/Route > Route List**.
- 2 Click **Add New** on the screen that appears.
- 3 In the **Route Group Configuration** screen, configure the following options:

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go

ccmadministrator Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Help

Route List Configuration Related Links: Back To Find/List Go

Save

Status
Status: Ready

Route List Information
Device is trusted
Name* Voice Mail SIP
Description Voice Mail SIP
Cisco Unified Communications Manager Group* Default

Save

- a In the **Name** field, enter a name for the **Route List**.
 - b Enter a description in the **Description** field.
 - c Set the **Cisco Unified Communications manager Group** to **Default**.
- 4 Click **Save**.
 - 5 Click **Add Route Group**.
 - 6 Select the Route Group created earlier in the **Route Group** drop down.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go

ccmadministrator Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Help

Route List Detail Configuration Related Links: Back To Find/List Go

Save

Status
Status: Ready

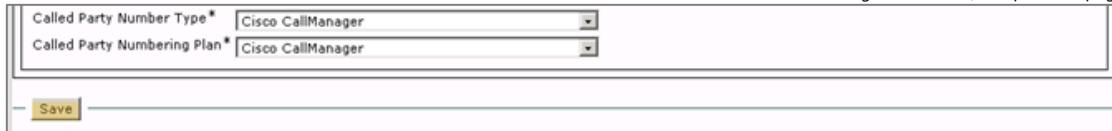
Route List Member Information
Route Group* Voice Mail SIP Route Group-[NON-QSIG]

Calling Party Transformations
Use Calling Party's External Phone Number Mask* Default
Calling Party Transform Mask
Prefix Digits (Outgoing Calls)
Calling Party Number Type* Cisco CallManager
Calling Party Numbering Plan* Cisco CallManager

Called Party Transformations
Discard Digits < None >
Called Party Transform Mask
Prefix Digits (Outgoing Calls)

Image continued on next page

Image continued from previous page

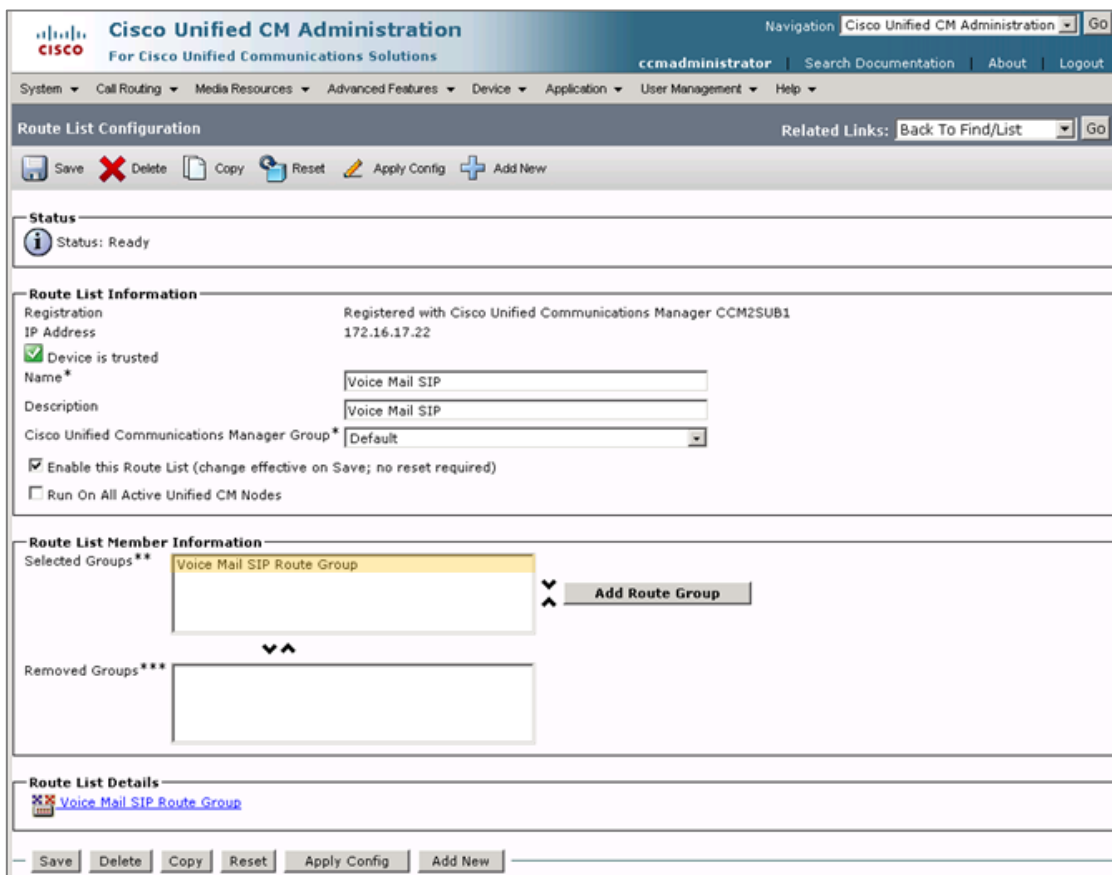


- 7 Click **Save**.

Verifying Route List Configuration

To Verify Route List Configuration:

- 1 In the **Route Group Configuration** screen, the Route Group should appear in the **Selected Groups** list.



- 2 If the Route Group does not appear on the list, perform the following steps to verify that it has made it to the list:
 - a In the **Related Links** field located in the upper-right corner, select **Back to Find/List** and press the **Go** button.
 - b On the next screen, press the **Find** button.
 - c In the result list, find and select the Route List that was created.
 - d The selected Route Group appears in the **Selected Groups** list.
- 3 Click **Save**.

Configuring Route Pattern

To Configure the Route Pattern:

- 1 Navigate to **Call Routing > Route/Hunt > Route Pattern**.
- 2 Click **Add New** on the screen that appears.
- 3 In the **Route Pattern Configuration** screen, configure the following options:

The screenshot shows the 'Route Pattern Configuration' page in the Cisco Unified CM Administration interface. The page has a navigation bar at the top with 'Cisco Unified CM Administration' and 'For Cisco Unified Communications Solutions'. Below the navigation bar is a 'Route Pattern Configuration' section with a 'Save' button and a 'Status' indicator showing 'Status: Ready'. The main configuration area is titled 'Pattern Definition' and contains the following fields and options:

- Route Pattern***: 5900
- Route Partition**: < None >
- Description**: Voice Mail SIP 5900
- Numbering Plan**: -- Not Selected --
- Route Filter**: < None >
- MLPP Precedence***: Default
- Resource Priority Namespace Network Domain**: < None >
- Route Class***: Default
- Gateway/Route List***: Voice Mail SIP (Edit)
- Route Option**:
 - ☒ Route this pattern
 - ☐ Block this pattern | No Error
- Call Classification***: OnNet
- ☐ Allow Device Override
- ☐ Provide Outside Dial Tone
- ☐ Allow Overlap Sending
- ☐ Urgent Priority
- ☐ Require Forced Authorization Code
- Authorization Level***: 0
- ☐ Require Client Matter Code

- a In the **Route Pattern** field, enter the hunt group directory number for the MiCollab AM Voice Mail system.
 - b In the **Description** field, enter a description.
 - c From the **Gateway/Route** list, select the Route List created earlier.
 - d Set **Call Classification** to **OnNet**.
 - e Deselect the **Provide Outside Dial Tone** checkbox.
- 4 Click **Save**.

Resetting SIP Trunk

Now that all configuration data has been entered, each trunk created needs to be reset.

To reset SIP trunk:

- 1 Navigate to **Device > Trunk**

- 2 Press **Find**.
- 3 For each new SIP trunk that was just added and configured:
 - Click on the trunk name to get to its corresponding configuration screen.
 - Press the **Reset** button
 - Press the **Reset** button on the pop-up screen
 - Press the **Close** button
 - Press the **Go** button in the upper-right corner next to the box that says Back to Find/List.
- 4 The trunks are now reset and should be able to service phone calls. The switch configuration is complete.

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: (1) Configuring MiCollab AM for the telephone system integration when you are installing MiCollab AM for the first time, or (2) Configuring the existing MiCollab AM with the new telephone system integration.

Click the appropriate steps that your system requires from below and follow the steps:

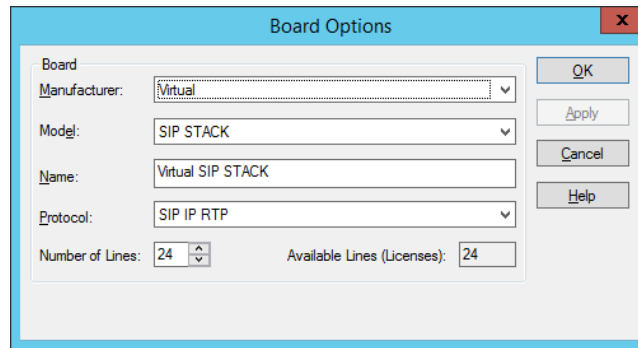
- [Configuring MiCollab AM for the Integration During Initial Installation](#): Integrate the telephone system while you install MiCollab AM for the first time.
- [Configuring Existing MiCollab AM for the Integration](#): Integrate a new telephone system on your existing MiCollab AM system.

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

Configuring MiCollab AM for the Integration During Initial Installation

To configure MiCollab AM for 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** dropdown list, select **Cisco**.
 - d From the **Model** dropdown list, select **Unified Communications Manager**.
 - e From the **Integration Type** dropdown list, select **SIP Trunk**.
- 2 Click **Next**. The **Board Options** dialog box appears.



The **Board Options** dialog box contains the following fields and controls:

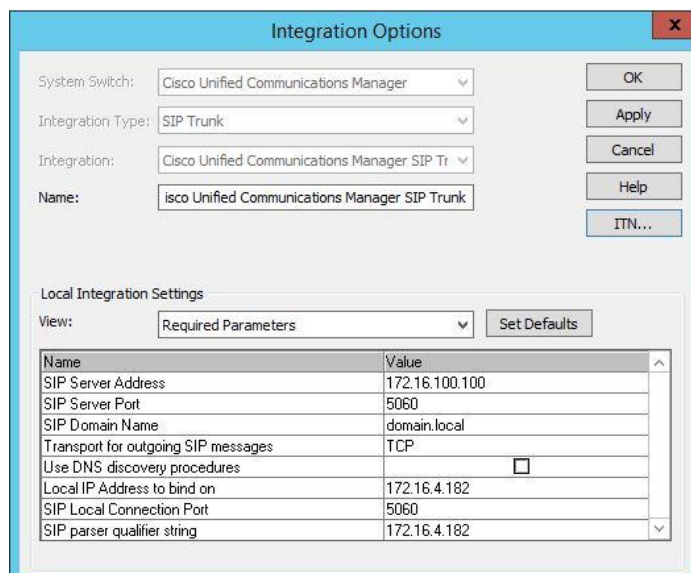
- Manufacturer:** Virtual (dropdown)
- Model:** SIP STACK (dropdown)
- Name:** Virtual SIP STACK (text field)
- Protocol:** SIP IP RTP (dropdown)
- Number of Lines:** 24 (spin box)
- Available Lines (Licenses):** 24 (spin box)
- Buttons: OK, Apply, Cancel, Help

- 3 In the **Board Options** dialog box, configure the following options:
 - a From the **Manufacturer** dropdown list, select **Virtual**.
 - b From the **Model** dropdown 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** dropdown 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.
- 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, refer to 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.



The **Integration Options** dialog box contains the following fields and controls:

- System Switch:** Cisco Unified Communications Manager (dropdown)
- Integration Type:** SIP Trunk (dropdown)
- Integration:** Cisco Unified Communications Manager SIP Trunk (dropdown)
- Name:** Cisco Unified Communications Manager SIP Trunk (text field)
- Buttons: OK, Apply, Cancel, Help, ITN...
- Local Integration Settings**
 - View:** Required Parameters (dropdown)
 - Set Defaults** (button)
 - Table:

Name	Value
SIP Server Address	172.16.100.100
SIP Server Port	5060
SIP Domain Name	domain.local
Transport for outgoing SIP messages	TCP
Use DNS discovery procedures	<input type="checkbox"/>
Local IP Address to bind on	172.16.4.182
SIP Local Connection Port	5060
SIP parser qualifier string	172.16.4.182

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

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

Table 4. Required Parameters View – Integration Options

Field	Required Value
SIP Server Address	Enter the FQDN or the IPv4/IPv6 IP address of the Cisco UCM
SIP Server Port	Enter the listening port of the Cisco UCM The default port number is 5060 . When configured for TLS , the port number is 5061 .
SIP Domain Name	Enter your LAN or VLAN domain (the domain in which both the Call Server and Cisco Unified Communication Manager reside).
Transport for outgoing SIP messages	This is the transport medium that will be used to send outgoing SIP messages. Select between UDP , TCP or TLS . The default is TCP .
Use DNS Discovery Procedures	Select this box if the SIP Server Address field is populated with an SRV record of the PBX. The default value of this field is disabled. NOTE If the SIP Server Address field is populated with the IP address or FQDN of the PBX, then enabling this field is not required.
Local IP Address to bind on	Select the IPv4/IPv6 IP address of the NIC on the MiCollab AM platform that should support the integration.
SIP Local Connection Port	Enter the port number where MiCollab AM listens for incoming SIP messages. The default value is 5060 . NOTE This parameter is used for non-TLS connections only.
SIP parser qualifier string	<ul style="list-style-type: none">• Single SIP integration on the call server: Enter the local IP address to which the integration is bound. This field is used by MiCollab AM to match SIP packets to the appropriate SIP integration.• Multiple SIP integrations on the call server: Use a string that is unique to each SIP integration. For example:<ul style="list-style-type: none">a. The extension that will be used as the hunt number on the PBX followed by the @ symbol and the IP of the call server, such as 5000@172.16.4.202. <i>The hunt number must be unique across all IP integrations.</i>

- b. The Fully Qualified Domain Name (FQDN) of the switch, such as pbx1.sipdomain.com.

NOTE This setting must match a string in the SIP header that is unique to this particular integration.

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

- In the **SIP Domain Name** field, enter your LAN or VLAN domain (the domain in which both the Call Server and Cisco Unified Communications Manager reside).
- Find **Type of Call Progress to use for External Calls** and set the value as how the gateway is used for the integration.

NOTE How this should be set depends on the gateway used for the integration.

- **Digital:** Select if the gateway supports call progress through to the endpoint.
- **Media:** Select if the gateway reports early that the call is connected, such as before the phone rings or while the phone is ringing.

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

- 9 In the **Switch Section Options** dialog box, configure the following options:

- a In the **Local Integration Settings** section, select the **Required Parameters** view.
- b In the **Hunt Group Access Code** field, enter the group pilot number you configured previously. This is the pilot number that users dial to reach MiCollab AM.
- c 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, configure callouts for the application. For information on configuring callout settings, see the topic *Configuring Callout Settings*, in the online help system.

- 13 Click **OK** to save all changes.

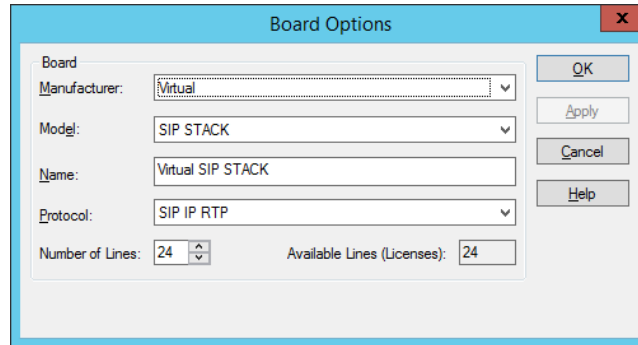
Configuring Existing MiCollab AM for the Integration

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** dropdown list, select **Virtual**.
 - b From the **Model** dropdown 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** dropdown 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 **Switches** tab and click the **Add** button. The **Switch Integration Data Setup** dialog box appears.
- a From the **Manufacturer** dropdown list, select **Cisco**.
 - b From the **Model** dropdown list, select **Unified Communications Manager**.
 - c From the **Integration Type** dropdown list, select **SIP Trunk**.
- 5 Click **OK**. The **Switch Options** dialog box appears.
- 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, refer to 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.

Integration Options

System Switch: Cisco Unified Communications Manager

Integration Type: SIP Trunk

Integration: Cisco Unified Communications Manager SIP Trunk

Name: Cisco Unified Communications Manager SIP Trunk

Local Integration Settings

View: Required Parameters

Name	Value
SIP Server Address	172.16.100.100
SIP Server Port	5060
SIP Domain Name	domain.local
Transport for outgoing SIP messages	TCP
Use DNS discovery procedures	<input type="checkbox"/>
Local IP Address to bind on	172.16.4.182
SIP Local Connection Port	5060
SIP parser qualifier string	172.16.4.182

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

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

Table 5. Required Parameters View – Integration Options

Field	Required Value
SIP Server Address	Enter the FQDN or the IPv4/IPv6 IP address of the Cisco UCM
SIP Server Port	Enter the listening port of the Cisco UCM The default port number is 5060 . When configured for TLS , the port number is 5061 .
SIP Domain Name	Enter your LAN or VLAN domain (the domain in which both the Call Server and Cisco Unified Communication Manager reside).
Transport for outgoing SIP messages	This is the transport medium that will be used to send outgoing SIP messages. Select between UDP , TCP or TLS . The default is TCP .
Use DNS Discovery Procedures	Select this box if the SIP Server Address field is populated with an SRV record of the PBX. The default value of this field is disabled. NOTE If the SIP Server Address field is populated with the IP address or FQDN of the PBX, then enabling this field is not required.
Local IP Address to bind on	Select the IPv4/IPv6 IP address of the NIC on the MiCollab AM platform that should support the integration.
SIP Local Connection Port	Enter the port number where MiCollab AM listens for incoming SIP messages. The default value is 5060 .

NOTE This parameter is used for non-TLS connections only.

SIP parser qualifier string

- **Single SIP integration on the call server:** Enter the local IP address to which the integration is bound. This field is used by MiCollab AM to match SIP packets to the appropriate SIP integration.
- **Multiple SIP integrations on the call server:** Use a string that is unique to each SIP integration.

For example:

- a. The extension that will be used as the hunt number on the PBX followed by the @ symbol and the IP of the call server, such as 5000@172.16.4.202. *The hunt number must be unique across all IP integrations.*
- b. The Fully Qualified Domain Name (FQDN) of the switch, such as pbx1.sipdomain.com.

NOTE This setting must match a string in the SIP header that is unique to this particular integration.

b In the **Local Integration Settings** section, select the **Integration Specific Parameters** View and configure the settings as follows:

- In the **SIP Domain Name** field, enter your LAN or VLAN domain (the domain in which both the Call Server and Cisco Unified Communications Manager reside).
- Find **Type of Call Progress to use for External Calls** and set the value as how the gateway is used for the integration.

NOTE How this should be set depends on the gateway used for the integration.

- **Digital:** Select if the gateway supports call progress through to the endpoint.
- **Media:** Select if the gateway reports early that the call is connected, such as before the phone rings or while the phone is ringing.

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

10 In the **Switch Section Options** dialog box, configure the following options:

- a In the **Local Integration Settings** section, select the **Required Parameters** view.
- b In the **Hunt Group Access Code** field, enter the group pilot number you configured previously. This is the pilot number that users dial to reach MiCollab AM.
- c 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 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** dropdown 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 6. Secondary SIP Server Address and the Secondary SIP Server Port example

Field	Value
Secondary SIP Server Address	<div>Enter the TCP/IP address or an FQDN of the secondary node.</div> <div>For example: The IP address 123.45.6.789 as displayed on the Review/Modify SIP Gateway screen.</div> <div>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.</div> <div>IMPORTANT This value must match the configuration on the Gateway of the secondary node.</div>
Secondary SIP Server Port	Enter the port number of the secondary node. The default value is 5060 .

- 7 From the **View** dropdown 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 following table.

Table 7. 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	<p>How this should be set depends on the gateway used for the integration.</p> <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** dropdown 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 MiCollab AM for TLS and SRTP

MiCollab AM can be configured for Transport Layer Signaling (TLS) and Secure Real-Time Transport Protocol (SRTP). Use the instructions provided in this section to add or remove TLS and SRTP.

IMPORTANT It is advised that you configure MiCollab AM to integrate with Cisco UCM using TCP initially to ensure that the integration is working prior to configuring MiCollab AM for TLS and SRTP communication.

This section assumes that you are familiar with preparing certificates for TLS communication which is not discussed in this document.

To configure TLS and SRTP settings:

- 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, configure the following options:
 - a In the **Local Integration Settings** section, select the **Required Parameters** view, and configure the following options:

The screenshot shows the 'Integration Options' dialog box. The 'System Switch' is set to 'Cisco Unified Communications Manager'. The 'Integration Type' is 'SIP Trunk'. The 'Integration' is 'Cisco Unified Communications Manager SIP Tr'. The 'Name' is 'Cisco Unified Communications Manager SIP Trunk'. The 'Local Integration Settings' section is expanded, showing the 'Required Parameters' view. The table below lists the settings and their values:

Name	Value
SIP Server Address	172.16.100.100
SIP Server Port	5061
SIP Domain Name	domain.local
Transport for outgoing SIP messages	TLS
Use DNS discovery procedures	<input type="checkbox"/>
Local IP Address to bind on	172.16.4.53
SIP Local Connection Port	5060
SIP parser qualifier string	172.16.4.53

Table 8. Required Parameters View

Field	Value
SIP Server Address	Enter the FQDN or the IPv4/IPv6 IP address of the Cisco UCM
SIP Server Port	Enter 5061 for TLS.

SIP Domain Name	Enter your LAN or VLAN domain (the domain in which both the Call Server and Cisco Unified Communication Manager reside).
Transport for outgoing SIP messages	Select TLS as the transport.
Local IP Address to bind on	Select the IPv4/IPv6 IP address of the NIC on the MiCollab AM platform that should support the integration.
SIP Local Connection Port	Enter the port number where MiCollab AM listens for incoming SIP messages. The default value is 5060 . NOTE This parameter is used for non-TLS connections only.
SIP parser qualifier string	<ul style="list-style-type: none"> • Single SIP integration on the call server: Enter the local IP address to which the integration is bound. This field is used by MiCollab AM to match SIP packets to the appropriate SIP integration. • Multiple SIP integrations on the call server: Use a string that is unique to each SIP integration. For example: <ol style="list-style-type: none"> a. The extension that will be used as the hunt number on the PBX followed by the @ symbol and the IP of the call server, such as 5000@172.16.4.202. <i>The hunt number must be unique across all IP integrations.</i> b. The Fully Qualified Domain Name (FQDN) of the switch, such as pbx1.sipdomain.com. NOTE This setting must match a string in the SIP header that is unique to this particular integration.

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

Table 9. Connection Security Settings

Field	Setting
Enable TLS	This parameter must be selected to enable TLS.
SIP Server Address	Enter the IP or FQDN of all of the Cisco UCM <div> NOTE You need to click Add Trusted SIP Server Address button for the SIP Server Address entry to be created. </div>
SIP Server TLS Port	Enter the port number used by Cisco UCM for SIP TLS connections.
SIP Local TLS Port	Enter the port number used by MiCollab AM for SIP TLS connections.
SSL/TLS protocol version	Select the SSL/TLS protocol version to be used. <div> NOTE To create secure connections, use TLS 1.3 (recommended where available) or 1.2 for the System Server and Call Servers. </div>
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. Select the MiCollab AM certificate you imported into the Windows certificates store for TLS communication and click OK .
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 Cisco UCM certificate and then click OK .

- c** In the **Local Integration Settings** section, select **Media Settings** view, and then configure the settings as follows:

Integration Options

System Switch: Cisco Unified Communications Manager

Integration Type: SIP Trunk

Integration: Cisco Unified Communications Manager SIP Tr

Name: Cisco Unified Communications Manager SIP Trunk

Local Integration Settings

View: Media Settings

Name	Value
Input volume shift from the phone line	0
Media encryption preference	SRTP only
Prefer RTP over SRTP	<input type="checkbox"/>
Encryption and Authentication algorithm preference	AES_CM_128_HMAC_SHA1_32
Transmit Master Key Identifier	<input type="checkbox"/>
Default size of the Master Key Identifier	4
Enable Key Derivation Rate	<input type="checkbox"/>
Key Derivation Rate	16
Window Size Hint	0

Table 10. Media Settings

Field	Setting
Media encryption preference	Select SRTP only

Encryption and Authentication algorithm preference	Select AES_CM_128_HMAC_SHA1_32
Transmit Master Key Identifier	This parameter must be cleared
Window Size Hint	This parameter must be set to 0

Changing the Network Binding Order on the MiCollab AM Platform

MiCollab AM uses the primary (public) network interface card (NIC) in the platform. 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.

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 document ensure that the binding order is correct when you set up the integration. However, 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. Refer to your operating system's documentation for details.

Table 11. 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