MiCollab Advanced Messaging
Avaya Communication Manager SIP Trunk With and Without Session Manager
Integration Technical Note

For version 9.2 and above

Mitel

1082-10430-6692
Rev 9.2.0.3.1 June 2021

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 2021, Mitel Networks Corporation

All rights reserved

Contents

Preface 5

References 5

Documentation 5

Documentation Updates 6

Help 6

Document Conventions 6

Features Supported by This Integration 7

Critical Application Considerations 10

Overview 13

Session Manager Based Integration 13

Installation Requirements 15

Telephone System Requirements 15

MiCollab AM Requirements 16

Programming the Telephone System 17

Preparing the Telephone System for the Integration 17

Assigning Node IP Addresses in the Communication Manger 17

Creating a SIP Signaling Group 18

Defining the IP Interfaces 20

Creating SIP Trunk Groups 21

Configuring the SIP Firewall 27

Configuring the Location 29

Creating an Adaptation 30

Configuring a SIP Entity 31

Configuring Entity Links 33

Configuring the Routing Policies 34

Configuring Dial Patterns 35

Creating a Hunt Group and Pilot Number 37

Creating a Coverage Path 38

Creating a Route Pattern 39

Modifying Digit Conversion Tables 40

Defining the Telephone System Location 41
Programming Subscriber Telephones 41
Verifying the Local Survivable Processor settings of Telephone System 46

Configuring MiCollab AM 50

Configuring MiCollab AM for the Integration During Initial Installation 50
Configuring Existing MiCollab AM for the Integration 54
Configuring MiCollab AM for SIP Failover 58

Changing the Network Binding Order on the MiCollab AM Platform 61

Windows Server 2012 R2 61
Windows Server 2016 / 2019 62

Configuring Quality of Service (QoS) 63

Preface

This Integration Technical Note (ITN) is written for MiCollab Advanced Messaging (MiCollab AM) certified technicians who are experienced with MiCollab AM and are familiar with its procedures and terminology. This document also assumes that you are familiar with the features and programming of the Avaya Aura Communication Manager Telephone system.

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	*System Administration Guide*
Server Documentation	*System Installation and Configuration Guide*
Online help	MiCollab AM online help system

Features Supported by This Integration

The following tables list the features supported using the Avaya Aura Communication Manager SIP Trunk 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 Avaya Aura Communication Manager SIP

Feature	Supported	Notes
Automatic subscriber logon	Yes	
ANI/CLI	Yes	

Announce Busy greeting on forwarded calls	Yes	
Call screening	Yes	Note 1
Caller queuing	Yes	Note 2
DNIS	Yes	
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	
Live record, integrated	No	
Live reply to sender	Yes	
Message notification callouts	Yes	
MWI, set/clear	Yes	
MWI, inband/outband	Outband	
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	
Silence Timeout	Yes	
SRTP	No	Note 3
TLS	No	Note 3
Transfers, blind	Yes	
Transfers, confirmed	Yes	
Transfers, fully supervised	Yes	
Transfers, monitored	Yes	

Trunk ID for call routing	No	
Multiple Integrations	Yes	Note 4

NOTES

1. Available only when using supervised transfers.
2. 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 Critical Application Considerations section.
3. MiCollab AM supports negotiation for SRTP media streams using the Secure RTP profile defined in RFC 3711 with the offer/answer model defined in RFC 3264. To enable SRTP, RTP, or both, see integration configuration options documentation for the switch. The default setting is RTP. Please note that MiCollab AM doesn't support RFC 5939 which is an extension of RFC 3264.

   To create secure connections, use TLS 1.3 (recommended where available) or 1.2 for the System Server and Call Servers.
4. Refer to the Critical Application Considerations section.

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.

- You must configure the **Hunt Group Access Code** in the **Switch Section Options** dialog box.
- 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.
- Multiple MiCollab AM Call Servers may be supported for this integration using the Mitel SIP Routing Manager. Please consult Mitel Technical Support for details.
- 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 SIP Domain Name in the **Integration Options** dialog box must match the domain name configured in the telephone system and on the TFTP server. This value is case sensitive.
- 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.

- 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 only to the specific Call Server on which their call is queued.
- If the Avaya H.323 telephones do not provide end-to-end DTMF to MiCollab AM, disable the system-wide parameter IP Shuffling in the System Parameters programming section of the Communication Manager. This is particularly important where multiple Avaya Medpro's are in use. Be sure the parameter, Hairpinning is enabled for all H.323 telephones and the SIP Signaling Group supporting MiCollab AM.

- In CM 5.2.1 and later releases, calls traversing SIP trunks must have the corresponding extensions administered in the appropriate private and public numbering tables of the public-unknown-numbering and private-numbering forms.
- If another application requiring a different configuration for G430 or G450 gateways will use Session Manager, a separate gateway will be required.
- Avaya Survivable Remote Server (formerly called Local Survivable Processor [LSP]) support – for Secondary or tertiary failover server scenarios.
  - SIP endpoints supported when defined to have the secondary Survivable Remote Server in Network region. Digital and Analog endpoints only supported if the reside within the G430 or G450 to which the Communication Manager has as set to be defined as the survivable server.

NOTE H.323 endpoints are not supported in a failover scenario.

  - For additional clarification on survivable server setup for the Avaya Communication Manager, see the following Avaya Documents:
    - *Deploying Avaya Aura Communication Manager* – Release 7.1.1 Issue 2
    - *Converting Avaya Servers and Gateways* (Document ID: 03-602884)
    - *Avaya Aura® Communication Manager Survivability Options* – Release 8.0 Issue 2
      - Know information on installing and configuring survivable core servers and migrating a main server to a survivable core server.
    - *Administering Network Connectivity on Avaya Aura Communication Manager* – Release 8.0 Issue 2
- Avaya Survivable Core Server (formerly called Enterprise Survivable Server [ESS]) support – for Secondary or tertiary failover server scenarios.
  - Each Survivable Core Server is administered on the main server, which can be either:
    - a S8500/S8700/S8800 Media Server
    - a server deployed on a VMWare environment (as of Avaya Communication Manager 6.0 and above)
    - a server deployed on the Avaya Appliance Virtualization Platform (AVP) (as of Avaya Communication Manager 7.1 and above)
  - The Avaya Survivable Core Server option is available from Avaya Communication Manager 3.0 and above and requires a software license for the main server and each Survivable Core Server to activate the Survivable Core Server feature. Configuration of Avaya equipment should be performed by Avaya and/or Avaya business partners.
- Direct IP-to-IP communication settings updates for Avaya Aura:
  - If the direct IP-to-IP setting is set as 'n', it will route calls directly through the Session Manager and bypass any MedPro configured on the TDM bus. This setting is also required to be used for TLS calls which will route through the Session Manager as well.
  - If the direct IP-to-IP setting is set as 'y' it will route the call through the TDM Bus (MedPro) resources.
  - When you are using the MedPro on the TDM bus as your IP resource, and you are calling between two SIP endpoints (when a SIP endpoint calls another SIP endpoint), the media stream will initially pass through a TDM resource.

However, once the call has been established and the TDM resource is no longer required, the call is "shuffled" away from the TDM bus and IP flows directly between the two SIP endpoints. This will Free up the TDM resource, releasing time-slots on the voice bus, and allow IP media to flow more efficiently

A few rules apply:

- Both SIP endpoints must be administered to allow shuffling. For Avaya phones, enable Intra-region IP-IP Direct Audio, Inter-region IP-IP Direct Audio, and IP Audio Hairpinning for the IP Network Region, and Direct-IP in System Features and the Signaling Group.
- The endpoints must be in the same LAN region or in interconnected LAN regions. The inter-region connection management rules must be met. There is at least one codec in common between the codec lists of the endpoints involved and the Internetwork region connection management codec list.
- The endpoints don't have to do anything special to initiate shuffling. It's all handled by the gateway. The endpoints will know when shuffling is occurring when they receive re-INVITE messages with new media descriptions.

- For additional clarification on network regions defined in the Avaya Communication Manager, see the following two Avaya Documents:
  - *Administering Network Connectivity on Avaya Aura Communication Manager* – Release 8.0 Issue 2
  - *Avaya Communication Manager Network Region Configuration Guide* (Document ID: 103244)

- MiCollab AM 9.2 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.

Overview

This document describes how to integrate MiCollab AM with an Avaya Aura Communication Manager Telephone system, using the Session Initiation Protocol (SIP) integration. This integration operates exclusively over an IP-based network. It uses no analog or digital voice telephony ports, but instead passes voice communication and signaling information over the network.

The Avaya Communication Manager SIP integration consists of the following major components:

- Avaya Aura Communication Manager
- Avaya Media Gateway
- Avaya Aura Session Manager Server (only when used for integration with MiCollab AM)

  NOTE There are two ways to configure Communication Manager SIP trunk. One is to use the Session Manager. The other is a direct SIP trunk configuration without the Session Manager. Configuration instructions throughout this document will indicate which configuration(s) will require the settings.

- Avaya Aura System Manager Server
- MiCollab AM

The integration process consists of configuring SIP support on the Media Gateway, configuring the telephone system at the gateway, configuring subscriber workstations, and configuring MiCollab AM. This document also describes the critical application considerations with which you should be familiar before you begin work on the integration.

Session Manager Based Integration

MiCollab AM integrates with Avaya Aura Communication Manager through the Session Manager using SIP trunks (referred to as SIP Entities on the Session Manager). Calls intended for MiCollab AM, whether direct or forwarded, are directed to this SIP trunk based on a dial pattern that matches the pilot number on the Avaya Communication Manager. The Call Server uses these same lines to place or transfer calls to the telephone system.

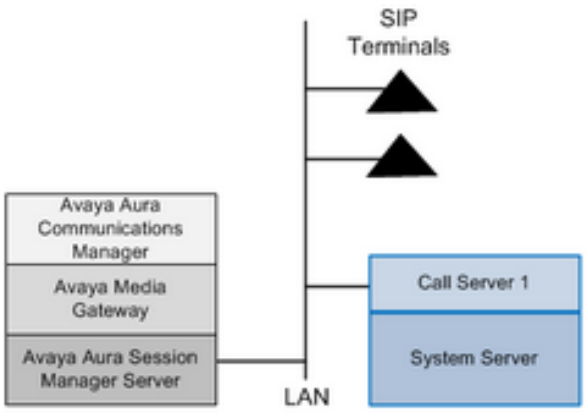


Figure 1. SIP Terminals

MiCollab AM sets and clears message waiting indicators (MWIs) by transmitting SIP messages to the Aura Session Manager server. As a result, MWI operations never restrict the number of lines available for calls.

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

- Avaya Aura Communication Manager 8.1 or prior

  NOTE If using Communication Manager 5.2.1, a patch to Communication Manager is required in order to add multiple Signaling Groups to a SIP Trunk Group for load balancing and failover support when using multiple MiCollab AM Call Servers.

  Without the patch, a separate SIP Trunk Group is required for each Call Server configured to overflow from one SIP Trunk Group/Call Server to the next. See the Avaya Communication Manager seed patch 18479 or contact your Avaya representative for more information.

  Note that the patch is service pack specific and Avaya may need to generate a patch for the specific service pack you have currently loaded or you may need to update Communication Manager to a service pack that already has a patch written for it.

  Note also that the system server programming instructions in this document assume the patch is loaded and the integration will use load balancing.

  IMPORTANT The above patch (18479) may no longer be available from Avaya which would limit the system to a single Call Server when integrating directly with Communication Manager (i.e., without Session Manager).

- Avaya Aura Session Manager 8.1 or prior, if Session Manager is being used.
- TN2302/TN2602 IP Media Processor with current firmware update, to handle voice processing tasks (or compatible hardware)
- TN799D C-LAN to process signaling information (or compatible hardware)
- One Administered SIP Trunk license per MiCollab AM port
- DSP Resources on Media Gateways (G430/G450) - Voice over IP (VoIP)

  NOTE The Avaya G Series Media Gateways features VoIP DSPs that provide voice services over IP data networks. The G450 features up to four VoIP DSPs and the G430 features up to two VoIP DSPs.

  These DSP resource modules allow you to use many types of telephones and trunks that do not directly support VoIP. The G450/G430 translates voice and signaling date between VoIP and the system used by the telephones and trunks as follows:

Avaya media modules convert the voice path of traditional circuits such as analog trunk, T1/E1, and DCP to a TDM bus inside the G450/G430.

The VoIP engine then converts the voice path from the TDM bus to a compressed or uncompressed and packetized VoIP on tan Ethernet connection. The G450/G30 provide VoIP service over the LAN and WAN.

The G450 supports up to four VoIP DSP childboards. Two types of childboard resource modules are supported, one providing 80 active VoIP channels and the other providing 20 active VoIP channels. The maximum number of active channels supported on the G450 is 240.

The G430 has an on-board VoIP DSP providing 20 VoIP channels, and supports an optional additional DSP board providing 10, 20, or 80 VoIP channels. The maximum number of active channels supported is 100.

All channels can be bi-directional FAX, G.711 u/A, G.726A, or G.729A/AB calls.

- Avaya Aura G430/G450 **Media Gateways** with S8300E for Survivable Remote Server (formerly LSP) failover server scenario. Survivable Remote Server (SIP endpoints supported in this configuration only)
- Avaya Communication Manager 3.0 and above with **S8500/S8700/S8800 Media Server** for Survivable Core Server (formerly ESS) failover server scenario
- Avaya Communication Manager 6.0 and above with VMWare environments for Survivable Core Server (formerly ESS) failover server scenario
- Avaya Communication Manager 7.1 and above with AVP environments for Survivable Core Server (formerly ESS) failover server scenario

MiCollab AM Requirements

- MiCollab AM version 9.2
- MiCollab AM software key diskette or feature file with the Avaya Communication Manager SIP integration enabled and one Virtual SIP and RTP license enabled for each port involved in the integration
- One 100 Mbps or 1000 Mbps (1 Gbps) network interface card

Programming the Telephone System

This section discusses programming the telephone system in a multiple call server environment. Follow the recommendations and programming examples in this section to program the telephone system for integration with MiCollab AM. Programming examples show commands and parameters that are necessary for integration; they do not represent PBX programming in its entirety. Settings that are critical to the integration appear in boldface.

The installing technician should be familiar with programming the telephone system. For detailed information on programming and installing the telephone system, refer to the Avaya documentation.

Preparing the Telephone System for the Integration

Before beginning the integration, make sure that the following configuration tasks are completed on the telephone system.

- Verify the PBX has enough Administered SIP Trunk licenses available for use with MiCollab AM
- Assigning IP node names and addresses to the components of the Communication Manager, and the Session Manager server platforms
- Defining IP interfaces
- Administering IP network regions

For more information on completing these tasks, refer to the documentation accompanying your telephone system.

Assigning Node IP Addresses in the Communication Manger

Assign the IP addresses on the Communication Manager. These IP address assignments are for communication between the Communication Manager, the Session Manager, and the gateway. Use the command, *change node-names ip* to assign the IP addresses required for the installation.

For the direct SIP integration, add the IP Address of the MiCollab AM Call Server. In this example, the call server name is **CXHACALL01**.

change node-names ip Page 1 of 2

IP NODE NAMES

Name	IP Address
AVAYACMSRV	172.16.20.122
CM-SimplexESS2	172.16.20.150
CStevenson	10.2.6.13
CX85LYNC01	172.16.5.10
CX87AVA	172.16.4.50
CXCALL05	172.16.4.221
CXECALL01CS	172.16.26.58
CXHACALL01	172.16.4.118
CXHACALL02	172.16.4.82
CXHASYSTEM	172.16.4.189
CXsipMeridian	172.16.4.65
CurtsSRM	172.16.7.161
Gateway001	172.16.20.1
IPOffice	172.16.21.101
Integautotest01	172.16.10.8
Integautotest02	172.16.10.6

(16 of 30 administered node-names were displayed)

Creating a SIP Signaling Group

Using the System Manager, go to **Elements** > **Communication Manager** > **Element Cut-Through** or a SAT terminal connection, and define a Signaling Group associating the Communication Manager and Session Manager servers, as shown in the following example.

To create SIP signaling group for every call server to be integrated:

1. **For the SIP trunk with Session Manager integration**:

   Specify a node name for the Session Manager and a listening port accessible to both the Session Manager and Communication Manager servers.

```
display signaling-group 99                                    Page   1 of   2
                              SIGNALING GROUP

 Group Number:  99              Group Type:  sip
  IMS Enabled?  n          Transport Method:    tls
        Q-SIP?  n
     IP Video?  n                                   Enforce SIPS URI for SRTP?    y
  Peer Detection Enabled?     n  Peer Server:    SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?      y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?      n
Alert Incoming SIP Crisis Calls?        n
   Near-end Node Name:  procr                  Far-end Node Name:  avayasip
 Near-end Listen Port:     5061                Far-end Listen Port:     5061
                                            Far-end Network Region:     1

Far-end Domain:    blvu.avstlabs.local
                                              Bypass If IP Threshold Exceeded?     n
Incoming Dialog Loopbacks:     eliminate                RFC 3389 Comfort Noise?    n
          DTMF over IP:  rtp-payload            Direct IP-IP Audio Connections?    n
Session Establishment Timer(min):       3                IP Audio Hairpinning?     n
          Enable Layer 3 Test?    y
                                                  Alternate Route Timer(sec):      6
```

```
display signaling-group 99                                    Page   2 of   2
                         LIMIT SIGNALING GROUP USAGE

                         Enable on the main Processor(s)?       y

          Enable on Survivable Processors (ESS and LSP):         all
```

For the Direct SIP trunk integration: Specify a node name for the MiCollab AM Call Server a listening port accessible to both the Call Server and Communication Manager servers.
In this example server **CXHACALL01**.

```
                                                              Page   1 of   2
                              SIGNALING GROUP

 Group Number:  57              Group Type:  sip
  IMS Enabled?  n          Transport Method:    tcp
        Q-SIP?  n
     IP Video?  n                                   Enforce SIPS URI for SRTP?    y
  Peer Detection Enabled?     y  Peer Server:    Others
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?      n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?      y
Alert Incoming SIP Crisis Calls?        n
   Near-end Node Name:  procr                  Far-end Node Name:  CXHACALL01
 Near-end Listen Port:     5060                Far-end Listen Port:     5060
                                            Far-end Network Region:

Far-end Domain:    blvu.avstlabs.local
                                              Bypass If IP Threshold Exceeded?     n
Incoming Dialog Loopbacks:     eliminate                RFC 3389 Comfort Noise?    n
          DTMF over IP:  rtp-payload            Direct IP-IP Audio Connections?    n
Session Establishment Timer(min):       3                IP Audio Hairpinning?     n
          Enable Layer 3 Test?    y
                                                  Alternate Route Timer(sec):      6
```

2 Specify the name of the domain on which the MiCollab AM platform is located.

3 Specify the **rtp-payload** method for the telephone system to use in transmitting DTMF tone sequences over the IP network.

4 Repeat this for each call server to be integrated. The *Group Number* on this screen is what will be entered for the Signaling Group later in this document.

Defining the IP Interfaces

IMPORTANT Be sure the Authoritative Domain name is the same throughout the Session Manager server, Communication Manager, and MiCollab AM programming.

To define the IP interfaces:

1 Log in to the System Manager, and go to **Elements** > **Routing** > **Domains**.

2 On the **Domain Management** page, click **New**. The options for adding a new domain display.

3 Fill in the options for domain name and type to define the IP Authoritative Domain and IP interfaces.

4 Add notes if necessary, and then click **Commit**.

5 In **Elements** > **Communication Manager** > **Element Cut-Through**, verify that the Authoritative Domain has been properly configured.

```
display ip-network-region 1                                   Page   1 of  20
                              IP NETWORK REGION
  Region:  1        NR Group:  1
Location:  1        Authoritative Domain:    blvu.avstlabs.local
     Name: NR 1                   Stub Network Region:    n
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio:        yes
       Codec Set:  1              Inter-region IP-IP Direct Audio:        yes
   UDP Port Min:  2048                      IP Audio Hairpinning?        y
   UDP Port Max:  3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value:     46
        Audio PHB Value:     46
        Video PHB Value:     26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority:       6
        Audio 802.1p Priority:       6
        Video 802.1p Priority:       5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled?   n
  H.323 Link Bounce Recovery?    y
 Idle Traffic Interval (sec):    20
   Keep-Alive Interval (sec):    5
             Keep-Alive Count:   5
```

Creating SIP Trunk Groups

Create the SIP Trunk Groups and populate them with the ports that support the MiCollab AM integration, as shown in the following two examples.

To create a SIP Trunk Group in a Single Call Server Environment, follow the second set of instructions below.

To create a SIP Trunk Group in a Single Call Server Environment:

1 Specify sip as the Group Type. Associate the new trunk group with the Signaling Group you created previously as follows:

For SIP trunk with Session Manager integrations:

```
                                                                    Page   1 of   21
                                    TRUNK GROUP

Group Number:  99                  Group Type:  sip            CDR Reports:  y
  Group Name:  SIP Features                COR:  1        TN:  1        TAC:  299
   Direction:  two-way        Outgoing Display?  n
 Dial Access?  n                                        Night Service:
Queue Length:  0
Service Type:  public-ntwrk            Auth Code?  n
                                                  Member Assignment Method:  auto
                                                           Signaling Group:  99
                                                         Number of Members:  99
```

```
                                                                    Page   5 of   21
                                    TRUNK GROUP
                                      Administered Members (min/max):      1/ 99
GROUP MEMBER ASSIGNMENTS                Total Administered Members:      99

      Port              Name
  1:  T01212            SIP Featur
  2:  T01213            SIP Featur
  3:  T01214            SIP Featur
  4:  T01215            SIP Featur
  5:  T01216            SIP Featur
  6:  T01217            SIP Featur
  7:  T01218            SIP Featur
  8:  T01219            SIP Featur
  9:  T01220            SIP Featur
 10:  T01221            SIP Featur
 11:  T01222            SIP Featur
 12:  T01223            SIP Featur
 13:  T01224            SIP Featur
 14:  T01225            SIP Featur
 15:  T01226            SIP Featur
```

For Direct SIP trunk integrations:

```
                                                                    Page   1 of  21
                                    TRUNK GROUP

Group Number:  27                  Group Type:  sip            CDR Reports:  y
  Group Name:  sip trunk - tcp              COR:  1        TN:  1        TAC:  227
   Direction:  two-way        Outgoing Display?  n
 Dial Access?  n                                     Night Service:
Queue Length:  0
Service Type:  tie                   Auth Code?  n
                                          Member Assignment Method:  auto
                                                   Signaling Group:  27
                                                 Number of Members:  20
```

```
                                                                    Page   2 of  21
      Group Type:  sip

TRUNK PARAMETERS

     Unicode Name:  auto

                                        Redirect On OPTIM Failure:  5000

           SCCAN? n                                Digital Loss Group:  18
                    Preferred Minimum Session Refresh Interval(sec):  1200

 Disconnect Supervision -     In?  y   Out?  y

            XOIP Treatment:  auto     Delay Call Setup When Accessed Via IGAR?  n

 Caller ID for Service Link Call to H.323 1xC:  station-extension
```

```
                                                                    Page   3 of  21
TRUNK FEATURES
          ACA Assignment?   n              Measured:   none
                                                          Maintenance Tests?    y


   Suppress # Outpulsing?    n   Numbering Format:   public
                                                   UUI Treatment:   service-provider

                                                    Replace Restricted Numbers?     n
                                                   Replace Unavailable Numbers?     n

                                                     Hold/Unhold Notifications?     y
                                     Modify Tandem Calling Number:     no



 Show ANSWERED BY on Display?  y
```

To create a SIP Trunk Group in a Multiple Call Server Environment:

1 Specify sip as the Group Type. Associate the new trunk group with the Signaling Group you created previously as follows:

For SIP trunk with multiple SIP trunk integrations and load balancing between them:

```
                                                                    Page   1 of  21
                                        TRUNK GROUP

Group Number:  53                  Group Type:  sip            CDR Reports:   y
  Group Name:  CXHACALL SIP                 COR:  1        TN:  1        TAC:  253
   Direction:  two-way        Outgoing Display?    n
 Dial Access?  n                                   Night Service:
Queue Length:  0
Service Type:  tie                   Auth Code?  n
                                          Member Assignment Method:   manual
```

```
                                                                  Page   5 of  21
                                   TRUNK GROUP
                                        Administered Members (min/max):      1/ 50
GROUP MEMBER ASSIGNMENTS                Total Administered Members:          50

      Port            Name                          Sig Grp
  1:  T00665          CXHACALL S                    53
  2:  T00666          CXHACALL S                    54
  3:  T00667          CXHACALL S                    53
  4:  T00668          CXHACALL S                    54
  5:  T00669          CXHACALL S                    53
  6:  T00670          CXHACALL S                    54
  7:  T00671          CXHACALL S                    53
  8:  T00672          CXHACALL S                    54
  9:  T00673          CXHACALL S                    53
 10:  T00674          CXHACALL S                    54
 11:  T00675          CXHACALL S                    53
 12:  T00676          CXHACALL S                    54
 13:  T00677          CXHACALL S                    53
 14:  T00678          CXHACALL S                    54
 15:  T00679          CXHACALL S                    53
```

NOTE You must build two separate signaling groups as well as two SIP trunk groups.

For direct SIP trunk integrations:

```
                                                                  Page   1 of  21
                                   TRUNK GROUP

Group Number:  53                  Group Type:  sip            CDR Reports:  y
  Group Name:  CXHACALL SIP                COR:  1        TN:  1        TAC:  253
   Direction:  two-way        Outgoing Display?  n
 Dial Access?  n                                   Night Service:
Queue Length:  0
Service Type:  tie                   Auth Code?  n
                                   Member Assignment Method:  manual
```

2 Ensure that the **Member Assignment Method** is set to **manual**.

3 Interleave the Signal Group member in **Sig Grp**.

For example:

> If you have two signal groups for two call servers, numbered 53 and 54, alternate these two number in the **Sig Grp** fields. If you have three call servers, enter a sequence of three.

4 On the Signaling Group form, set **Enable Layer 3 Test** to y.

```
                                                                  Page   1 of   2
                                  SIGNALING GROUP

  Group Number: 53                 Group Type: sip
   IMS Enabled?  n            Transport Method:  tcp
         Q-SIP?  n
      IP Video?  n                                      Enforce SIPS URI for SRTP?    y
   Peer Detection Enabled?     y   Peer Server:    Others
  Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?        n
 Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?        y
 Alert Incoming SIP Crisis Calls?        n
    Near-end Node Name:  procr                   Far-end Node Name:  CXHACALL01
  Near-end Listen Port:  5060                  Far-end Listen Port:  5060
                                            Far-end Network Region:  1

 Far-end Domain:  blvu.avstlabs.local
                                                Bypass If IP Threshold Exceeded?    n
 Incoming Dialog Loopbacks:     eliminate                RFC 3389 Comfort Noise?    n
           DTMF over IP:  rtp-payload             Direct IP-IP Audio Connections?    n
 Session Establishment Timer(min):       3                 IP Audio Hairpinning?    n
           Enable Layer 3 Test?  y
                                                     Alternate Route Timer(sec):    6
```

```
                                                                  Page   1 of   2
                                  SIGNALING GROUP

  Group Number: 54                 Group Type: sip
   IMS Enabled?  n            Transport Method:  tcp
         Q-SIP?  n
      IP Video?  n                                      Enforce SIPS URI for SRTP?    y
   Peer Detection Enabled?     y   Peer Server:    Others
  Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?        n
 Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?        y
 Alert Incoming SIP Crisis Calls?        n
    Near-end Node Name:  procr                   Far-end Node Name:  CXHACALL02
  Near-end Listen Port:  5060                  Far-end Listen Port:  5060
                                            Far-end Network Region:  1

 Far-end Domain:  blvu.avstlabs.local
                                                Bypass If IP Threshold Exceeded?    n
 Incoming Dialog Loopbacks:     eliminate                RFC 3389 Comfort Noise?    n
           DTMF over IP:  rtp-payload             Direct IP-IP Audio Connections?    n
 Session Establishment Timer(min):       3                 IP Audio Hairpinning?    n
           Enable Layer 3 Test?  y
                                                     Alternate Route Timer(sec):    6
```

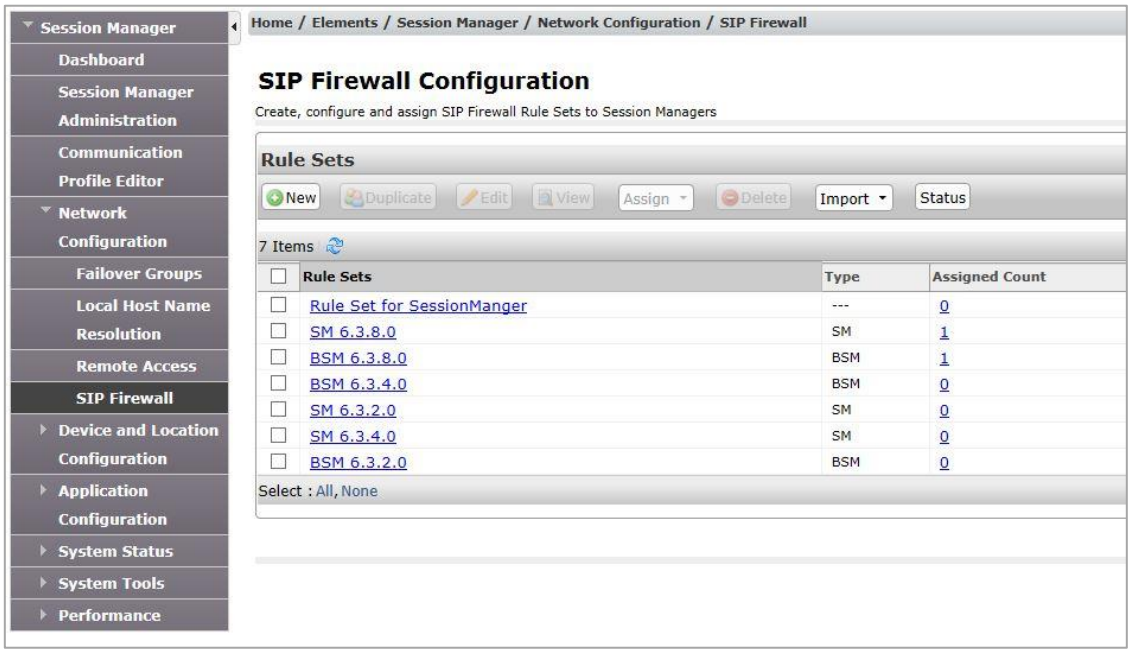
Configuring the SIP Firewall

NOTE This section is not required for Direct SIP trunk integrations.

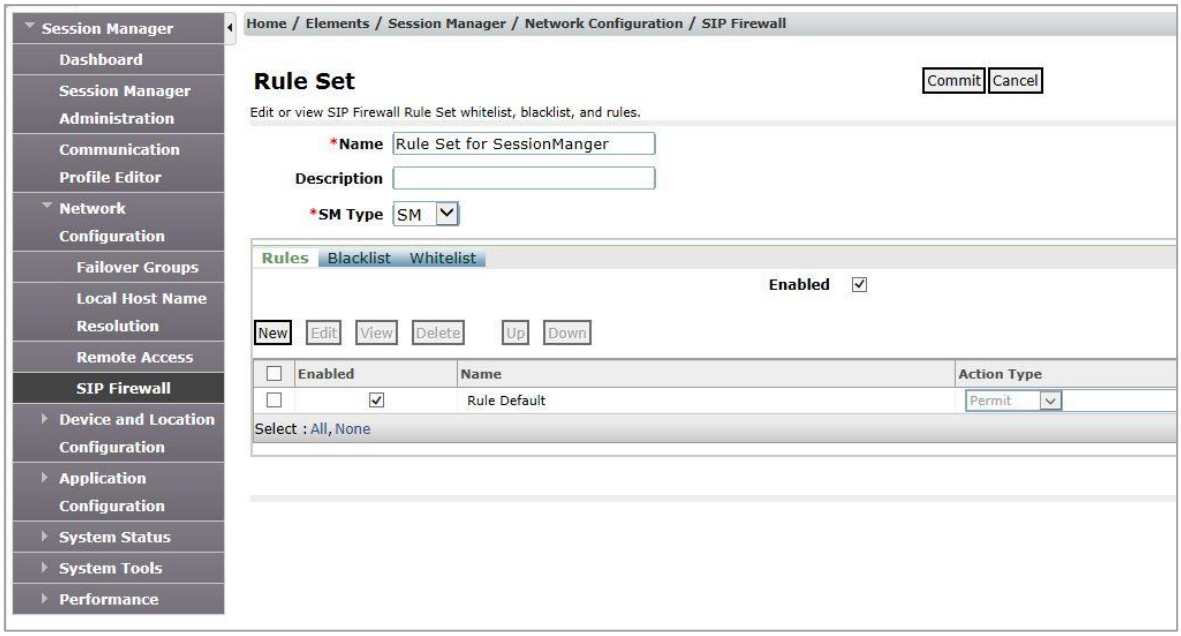
Configure the SIP firewall and ensure the MiCollab AM server's IP address is not blocked by the Session Manager firewall.

To add and configure the firewall to allow access to the MiCollab AM server's IP address:

1 Log in to the System Manager, and go to **Elements** > **Session Manager** > **Network Configuration** > **SIP Firewall**. The **SIP Firewall Configuration** page appears.

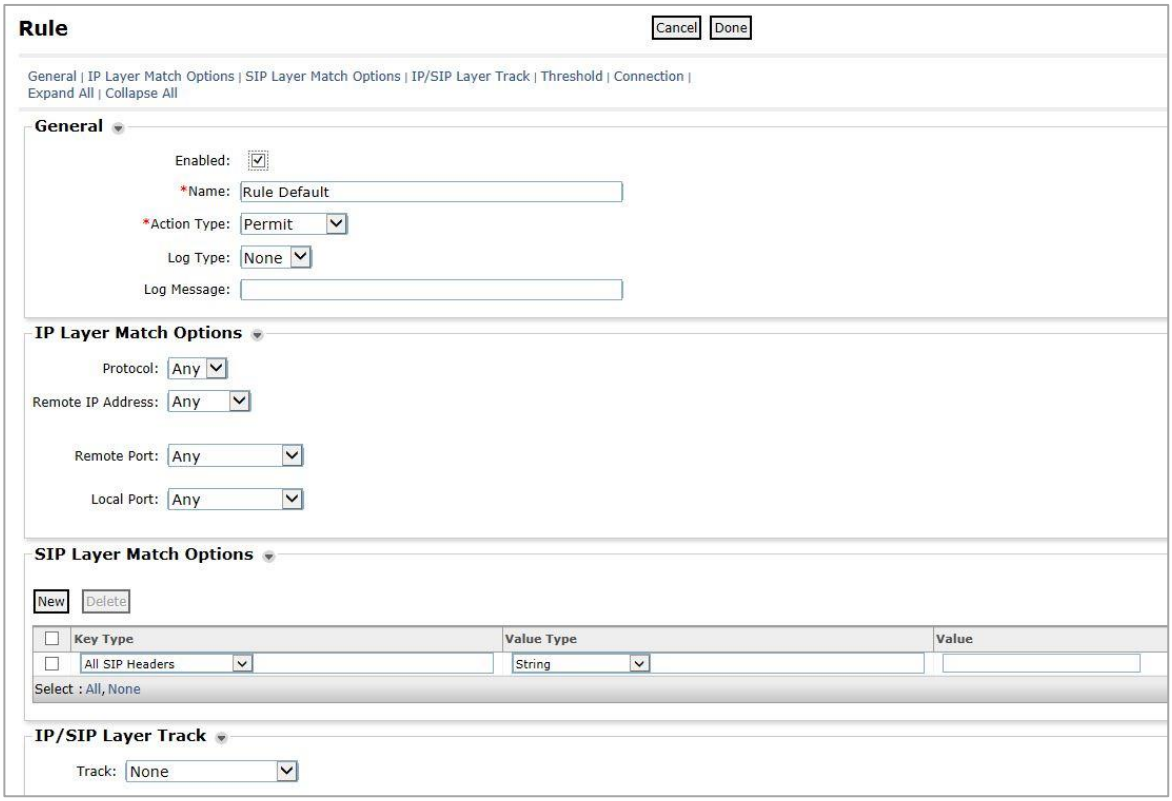


2 On the **SIP Firewall Configuration** page, in the **Rule Sets** section, click **New**. The **Rule Set** page appears.



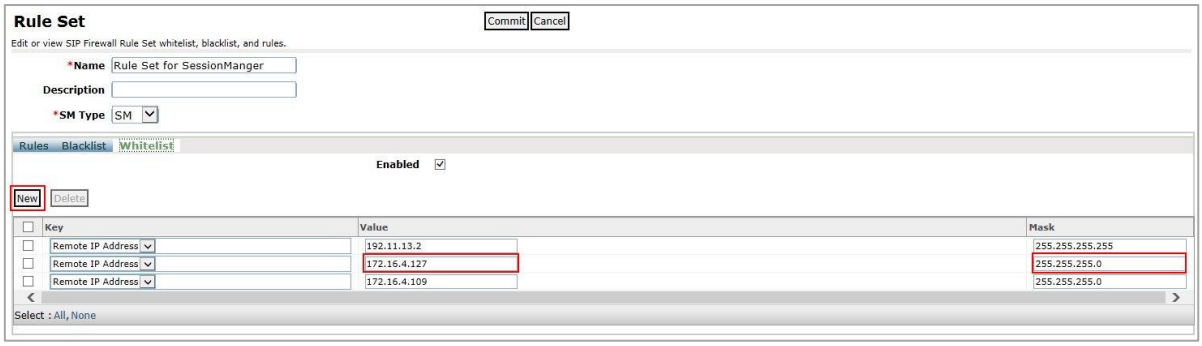
3 In the **Name** field, select or type *Rule Set for SessionManager*.

4 In the **Rules** tab, click **New**. The **Rule** page appears.



5 On the **Rule** page, fill the appropriate options in order for the firewall to allow access to the MiCollab AM server's IP address. When finished, click **Done**.

6 Click the **Whitelist** tab, and then click **New**.



7 Define an IP address to ensure that an IP address is not being blocked by a firewall. Click **Commit**.

Configuring the Location

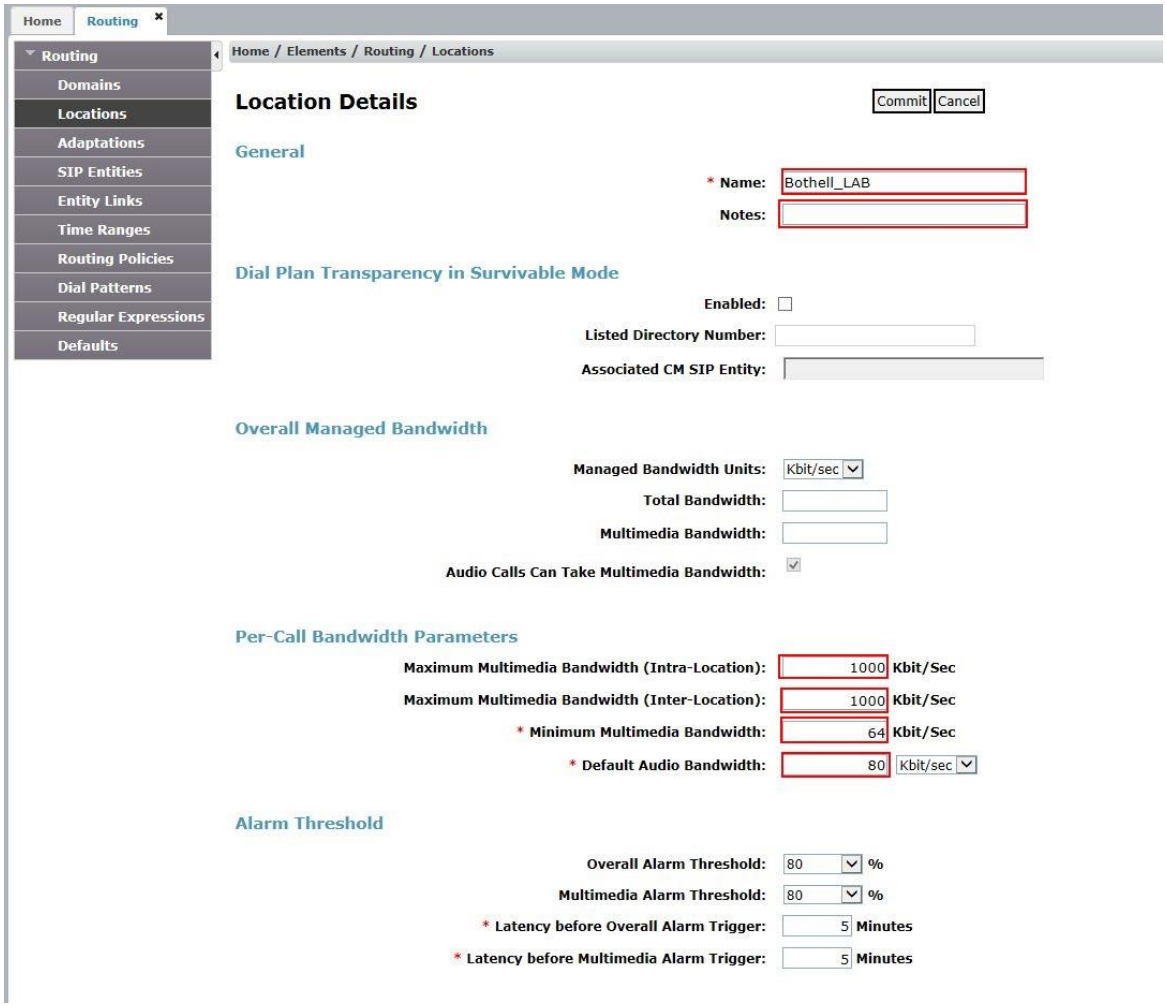
NOTE This section is not required for Direct SIP trunk integrations.

Session Manager uses locations to determine which dial patterns to look when routing a call. Each SIP entity has a particular IP address. Depending on the physical and geographic location of each SIP entity, some of the SIP entities can be grouped into a single location. You may use an already existing suitable location for MiCollab AM or create a new one.

To create a Location:

1 Log in to the System Manager, and go to **Elements** > **Routing** > **Locations**.

2 On the **Locations** page, click **New** to create a new location. The **Location Details** page appears. This location is used to create a SIP Entity for the MiCollab AM Call Server.



3 In the **General** section:

   a In the **Name** field, enter a name for the location.

   b (Optional) In the **Notes** field, enter a descriptive note that helps identify the location.

4 In the **Per-Call Bandwidth Parameters** section, enter a value based on the site policies (the default is blank).

> **For example:**
>
> G.711 Mu law uses roughly 80kbps of bandwidth per call.

5 In the **Location Pattern** section, enter a pattern that allows the MiCollab AM Call Server IP address.

6 Click **Commit** to save the changes.

Creating an Adaptation

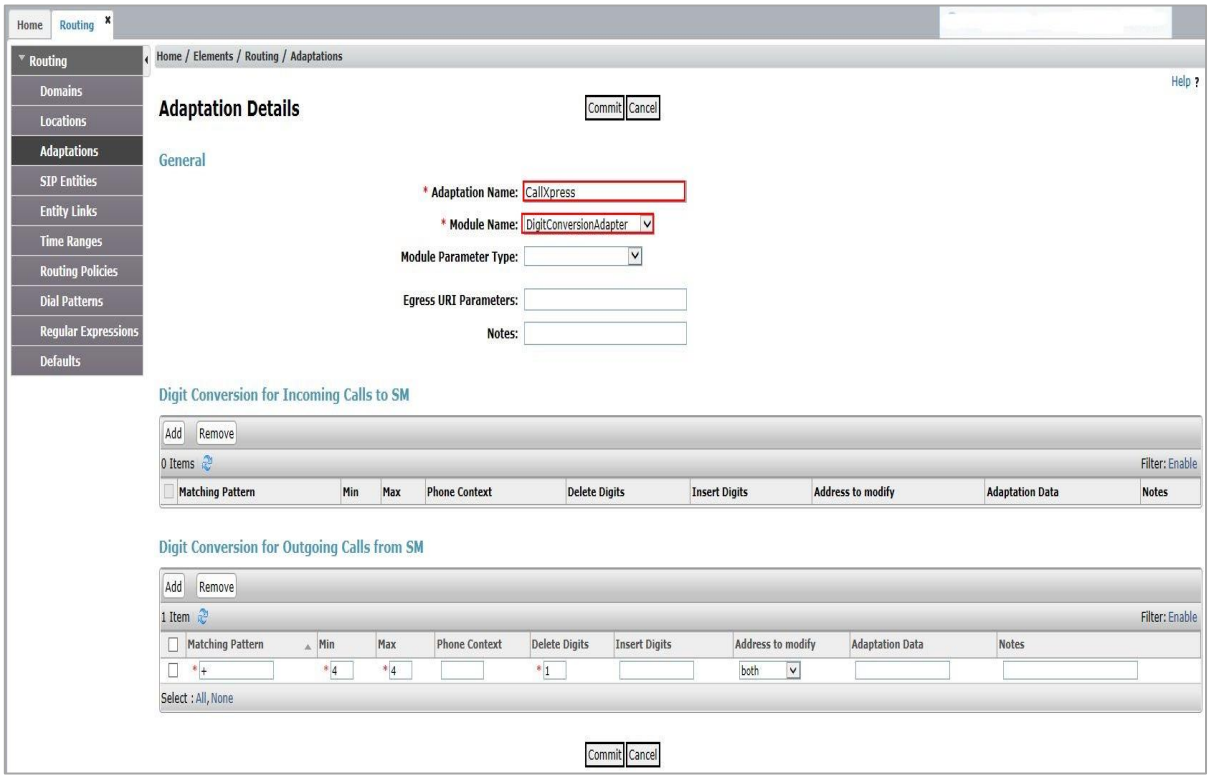
NOTE This section is not required for Direct SIP trunk integrations.

Adaptations modify the SIP messages that leave the Session Manager. The associated adaptation is used when routing calls to the SIP Entity.

To create an Adaptation:

1 Log in to the System Manager, and go to **Elements** > **Routing** > **Adaptations**.

2 On the **Adaptations** page, click **New** to create a new adaptation. The **Adaptations Details** page appears.



3 In the **General** section:

   a In the **Adaptation Name** field, enter an Adaptation name.

   b In the **Module Name** field, select **DigitConversionAdapter** from the list.

   c The remaining fields can retain their default values.

4 Click **Commit** to save the changes.

Configuring a SIP Entity

NOTE This section is not required for Direct SIP trunk integrations.

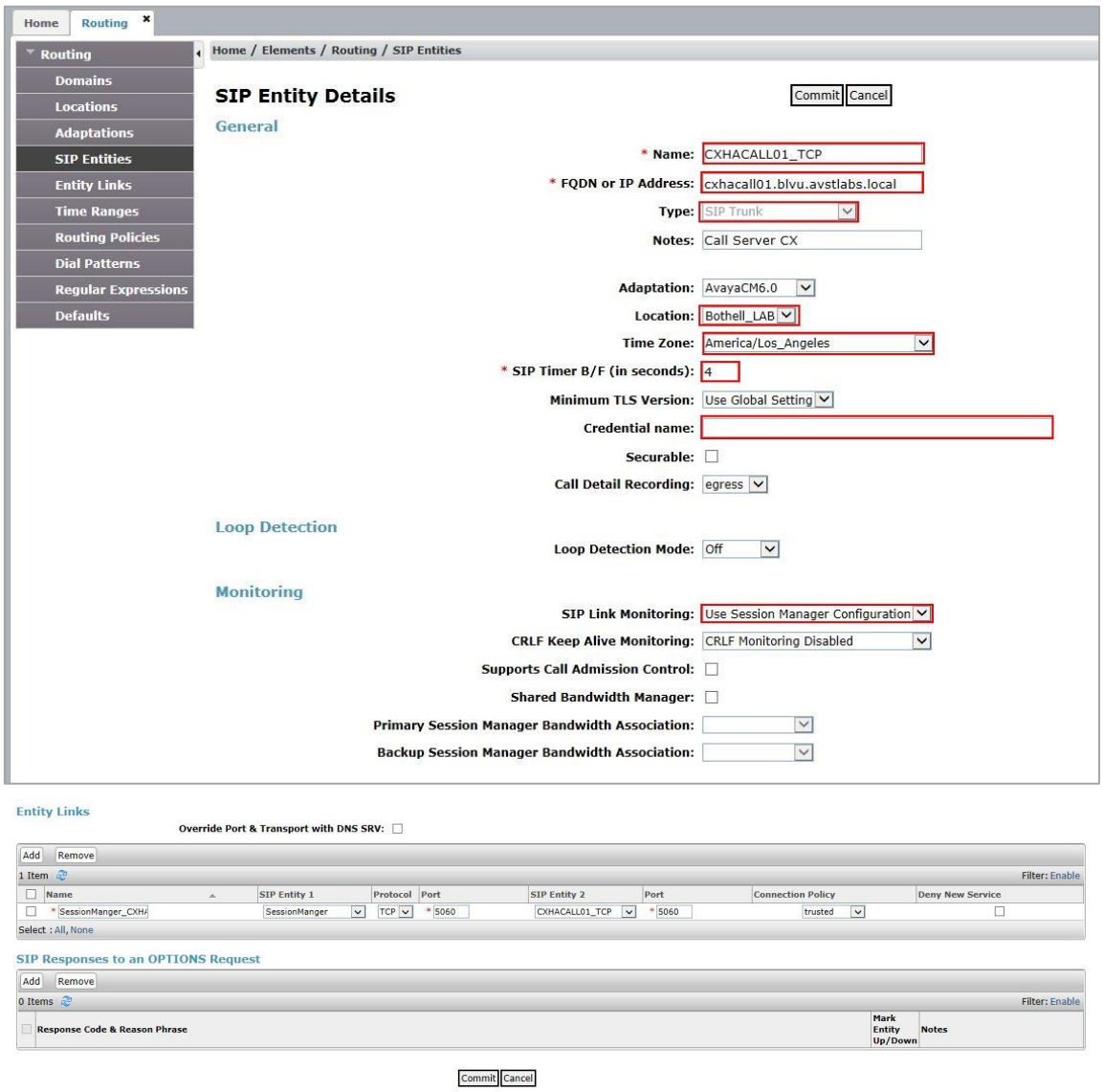
SIP Entities are all network entities that are part of the SIP domain. Verify all of the IP connections between the Communications Manager and Session Manager servers on the Session Manager server and make sure the Communication Manager server Interface reflects the same IP addresses as the Media Server Interface.

Create a SIP entity for MiCollab AM. The Session Manager uses a SIP Entity to route calls to the Call Server.

NOTE For more information on SIP Entities, refer to the Avaya document 03-603324. See the topic, *Administering Avaya Aura Session Manager*.

To create a SIP Entity:

1. Log in to the System Manager, and go to **Elements** > **Routing** > **SIP Entities**.
2. On the **SIP Entities** page, click **New** to create a new SIP Entity for MiCollab AM Call Server. The **SIP Entity Details** page appears.



3. In the **General** section:
   - **a** In the **Name** field, enter a unique name for the SIP Entity.
   - **b** In the **FQDN or IP Address** field, enter the fully qualified domain name or IP address of the SIP entity.

c In the **Type** field, select **SIP Trunk** from the list.

d (Optional) In the **Notes** field, enter a descriptive note that helps identify the SIP Entity.

e In the **Location** field, select a SIP entity location from the list (previous defined).

f In the **Outbound Proxy** field, specify a proxy if the entity type is Session Manager and you wish to specify it.

g In the **Time Zone** field, select the default time zone to be used for the entity.

h In the **Credential name** field, enter the credential name that is used for TLS connection validation by searching for this string in the SIP entity identity certificate.

- If you do not want to perform the additional validation on the SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
- If you want to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax.
- If you want to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax.

4 In the **SIP Link Monitoring** section, select **Use Session Manager Configuration** from the list.

NOTE This selection uses the settings from **Elements** > **Session Manager** > **Session Manager Administration** > **Session Manager Instances (Edit)** > **Monitoring**. If monitoring is disabled, then the administrator should select **Link Monitoring Enabled** from the list in step 12. The default values may be changed based on the site policy.

5 Click **Commit** to save the changes.

Configuring Entity Links

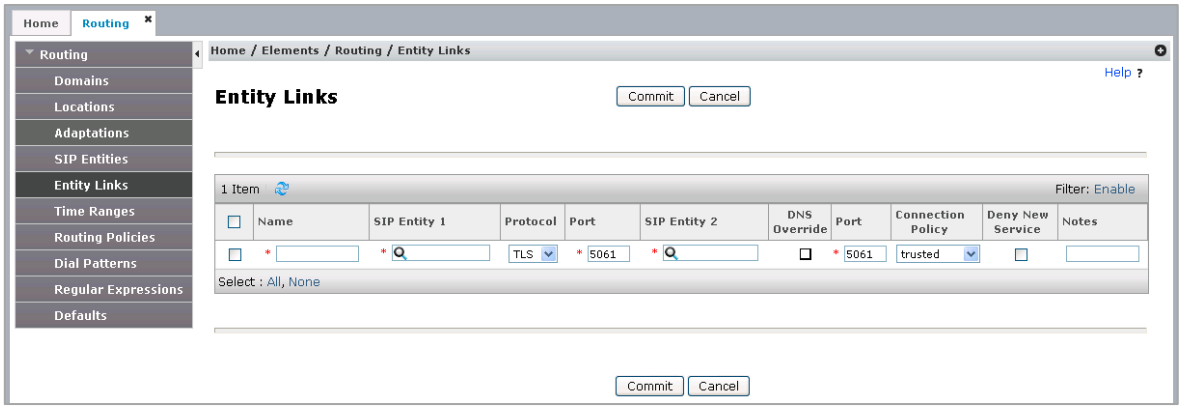
NOTE This section is not required for Direct SIP trunk integrations.

Configure an entity link for the Session Manager that allows it to send and receive messages with MiCollab AM.

To configure the Entity Link:

1 Log in to the System Manager, and go to **Elements** > **Routing** > **Entity Links**.

2 On the **Entity Links** page, click **New** to create a new Entity Link between the Session Manager and MiCollab AM Call Server. The **Entity Links** page appears.



3 In the **Name** field, enter a Name for the Entity Link.

4 In the **SIP Entity 1** field, select **Session Manager** from the list.

5 In the **Protocol** field, select **TCP** from the list.

6 In the **Port** field, enter **5060**.

7 In the **SIP Entity 2** field, select the SIP Entity you created for MiCollab AM in the previous procedure from the list, in this example, *Buffalo*.

8 In the **Port** field, enter **5060**.

> **NOTE** This port number must match the listening port configured on MiCollab AM in the **Integrations Options** dialog box.

9 Select the **Trusted** checkbox to make the Entity Link trusted.

10 (Optional) In the **Notes** field, enter a description for identification.

11 Click **Commit** to save changes.

Configuring the Routing Policies

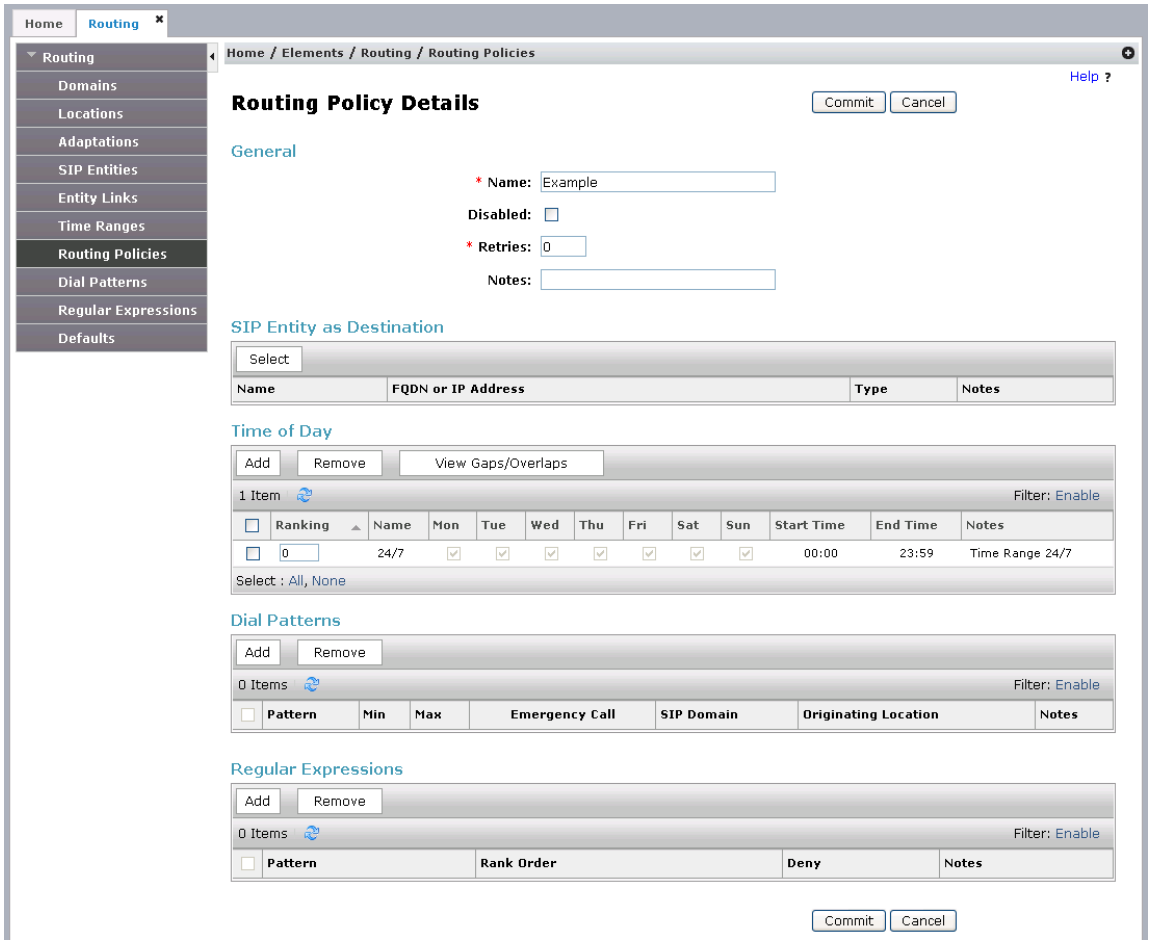
> **NOTE** This section is not required for Direct SIP trunk integrations

Configure the routing policies associated with the SIP Entity created for MiCollab AM.

To configure the routing policies:

1 Log in to the System Manager, and go to **Elements** > **Routing** > **Routing Policies**.

2 On the **Routing Policies** page, click **New** to create a new Routing Policy. The **Routing Policy Details** page appears.



3 In the **General** section:

   a In the **Name** field, enter a name for the policy.

   b (Optional) In the **Notes** field, enter a descriptive note for identification.

4 In the **SIP Entity as Destination** section, click **Select**.

   a From the SIP Entities page, select the SIP Entity created previously for MiCollab AM.

   b Click **Select**.

5 In the **Time of Day** section, adjust the **Time of Day per site policies** or keep the default values.

6 Click **Commit** to save the changes.

Configuring Dial Patterns

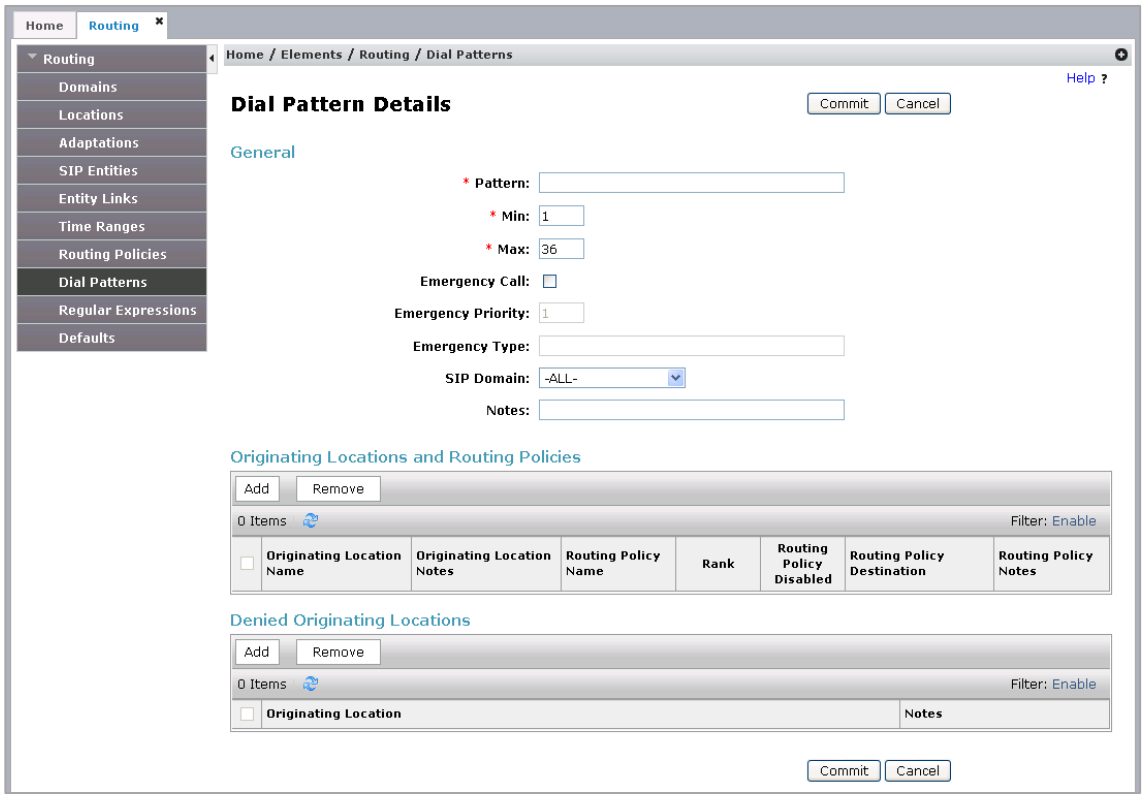
NOTE This section is not required for Direct SIP trunk integrations

Configure a dial pattern to route calls to MiCollab AM based on the dialed digits.

To configure a Dial Pattern:

1 Log in to the System Manager, and go to **Routing** > **Dial Patterns**.

2 On the **Dial Patterns** page, click **New** to create a new Dial Pattern. The **Dial Patter Details** page appears.



3 In the **General** section:

- **a** In the **Pattern** field, enter a pattern that allows calls directed to the MiCollab AM hunt group number to be routed to MiCollab AM.

  > **For example:**
  > A pattern that matches the Hunt group number.

  NOTE The pattern can be 1 to 36 digits long. A valid pattern format is '[+*#0-9x][0-9x]{0,35}'.

- **b** In the **Min** field, enter the minimum number of matching digits.
- **c** In the **Max** field, enter the maximum number of matching digits.
- **d** In the **SIP Domain** field, select the SIP Domain to which this dial pattern should be restricted. You may allow it for all SIP Domains.
- **e** (Optional) In the **Notes** field, enter a descriptive note for identification.

4 In the **Originating Location Name** section:

- **a** Click **Add** to add an Originating Location and a Routing Policy.
- **b** In the **Originating Location** section, select a location from the list of Originating Locations.
- **c** In the **Routing Policy** section, select the Routing Policy that you created previously.
- **d** Click **Select**.

5 Returns to the **Dial Pattern** page. Click **Commit** to save the changes.

Creating a Hunt Group and Pilot Number

From the System Manager, go to **Elements** > **Communication Manager** > **Element Cut-Through** and create a hunt group for MiCollab AM and assign it a pilot number. This number must match the previously defined Dial Pattern number. The following examples show typical hunt group configuration for this integration.

```
                                                          Page   1 of   60
                                 HUNT GROUP

           Group Number:  57                                ACD? n
             Group Name:  CX_HACALL01_TCP                 Queue? n
        Group Extension:  5700                           Vector? n
             Group Type:  ucd-mia                 Coverage Path:
                     TN:  1            Night Service Destination:
                    COR:  1                     MM Early Answer? n
          Security Code:                   Local Agent Preference? n
  ISDN/SIP Caller Display:  grp-name
```

```
                                                          Page   2 of   60
                                 HUNT GROUP



                     Message Center:   sip-adjunct

   Voice Mail Number        Voice Mail Handle        Routing Digits
                                                   (e.g., AAR/ARS Access Code)
   5700                       5700                       107
```

```
                                                                    Page   3 of   60
                                    HUNT GROUP
          Group Number:  57    Group Extension:    5700          Group Type:  ucd-mia
  Member Range Allowed: 1 - 1500          Administered Members (min/max):     0    / 0
                                              Total Administered Members:     0
GROUP MEMBER ASSIGNMENTS
     Ext            Name(19 characters)        Ext            Name(19 characters)
   1:                                        14:
   2:                                        15:
   3:                                        16:
   4:                                        17:
   5:                                        18:
   6:                                        19:
   7:                                        20:
   8:                                        21:
   9:                                        22:
  10:                                        23:
  11:                                        24:
  12:                                        25:
  13:                                        26:

  At End of Member List
```

Creating a Coverage Path

Define a Coverage Path to use on all MiCollab AM subscriber extensions, as shown in the following example. In this Coverage Path (57), define the MiCollab AM hunt group (57) as the only Coverage Point. Configure the Coverage Path so that the telephone system forwards calls to this Coverage Point when a subscriber extension is busy, ring-no-answer (RNA), or set to do-not-disturb mode (DND).

```
                              COVERAGE PATH

                 Coverage Path Number:   57
   Cvg Enabled for VDN Route-To Party?    n        Hunt after Coverage?    n
                     Next Path Number:            Linkage

COVERAGE CRITERIA
    Station/Group Status      Inside Call      Outside Call
              Active?            n                n
                Busy?            y                y
          Don't Answer?          y                y          Number of Rings:   2
                All?             n                n
   DND/SAC/Goto Cover?           y                y
     Holiday Coverage?           n                n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances?          n
  Point1:   h57              Rng:     Point2:
  Point3:                             Point4:
  Point5:                             Point6:
```

Creating a Route Pattern

Define a call routing pattern as shown in the following example. Associate this pattern with the trunk group you defined earlier.

IMPORTANT You must deactivate Secure SIP in this route pattern.

Example for SIP trunk with SM integrations:

```
                                                                  Page   1 of   3
                    Pattern Number:   99      Pattern Name:   SIP_Features
   SCCAN? n     Secure SIP?   n      Used for SIP stations?     n

   Grp  FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
   No            Mrk Lmt List Del  Digits                               QSIG
                                Dgts                                    Intw
 1: 1     0                                                              n    user
 2:                                                                      n    user
 3:                                                                      n    user
 4:                                                                      n    user
 5:                                                                      n    user
 6:                                                                      n    user

     BCC VALUE   TSC CA-TSC     ITC BCIE Service/Feature PARM Sub   Numbering LAR
    0 1 2 M 4 W       Request                                      Dgts Format
 1: y y y y y n   n              rest                                 unk-unk     none
 2: y y y y y n   n              rest                                             none
 3: y y y y y n   n              rest                                             none
 4: y y y y y n   n              rest                                             none
 5: y y y y y n   n              rest                                             none
 6: y y y y y n   n              rest                                             none
```

Example for the Direct SIP trunk integration:

```
                                                                    Page   1 of   3
                    Pattern Number:   57      Pattern Name:   CXHACALL01
  SCCAN? n     Secure SIP?   n      Used for SIP stations?      n

  Grp  FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
  No            Mrk Lmt List Del  Digits                                QSIG
                                  Dgts                                  Intw
1: 57   0                                                                n    user
2:                                                                       n    user
3:                                                                       n    user
4:                                                                       n    user
5:                                                                       n    user
6:                                                                       n    user

    BCC VALUE   TSC CA-TSC     ITC BCIE Service/Feature PARM Sub   Numbering LAR
    0 1 2 M 4 W      Request                                       Dgts Format
1: y y y y y n   n             rest                                            none
2: y y y y y n   n             rest                                            none
3: y y y y y n   n             rest                                            none
4: y y y y y n   n             rest                                            none
5: y y y y y n   n             rest                                            none
6: y y y y y n   n             rest                                            none
```

Modifying Digit Conversion Tables

Update the Automatic Alternate Routing (AAR) digit analysis table so that the pilot number is a valid dialed string that maps to the route pattern you have defined for the MiCollab AM pilot number, as shown in the following example.

```
                                                                    Page   1 of   2
                          AAR DIGIT ANALYSIS TABLE
                                Location:   all              Percent Full:   1

      Dialed          Total      Route    Call   Node   ANI
      String        Min   Max   Pattern   Type   Num    Reqd
      5               7     7    999      aar           n
      5030            4     4    1        aar           n
      51              4     4    88       aar           n
      5300            4     4    53       aar           n
      5400            4     4    54       aar           n
      5500            4     4    27       aar           n
      5600            4     4    1        aar           n
      5700            4     4    57       aar           n
      5800            4     4    58       aar           n
      5900            4     4    59       aar           n
      6               7     7    999      aar           n
      6000            4     4    99       unku          n
      7               7     7    999      aar           n
      7000            4     4    99       aar           n
      8               7     7    999      aar           n
```

Update the AAR digit conversion table so that all ranges of extension numbers used for MiCollab AM integration ports and subscriber extensions are defined as valid extension patterns, as shown in the following example.

Page 1 of 2

AAR DIGIT CONVERSION TABLE

Location: all Percent Full: 0

Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	ANI Req
5	4	4	0		ext	y	n
6	4	4	0		ext	n	n
8	4	4	0		ext	n	n
x11	3	3	0		ars	y	n
							n
							n
							n
							n
							n
							n
							n

Defining the Telephone System Location

Update the location definition as shown in the following example, so that the definition specifies the route pattern you defined earlier.

change locations Page 1 of 1

LOCATIONS

ARS Prefix 1 Required For 10-Digit NANP Calls? y

Loc No	Name	Timezone Offset	DST	City/ Area	Proxy Sel Rte Pat
1	Main	+ 00 : 00	0	425	1

Programming Subscriber Telephones

Subscriber telephone programming involves setting up initialization parameters for SIP-based telephones and configuring the corresponding extensions in the telephone system.

NOTE There are several ways to setup initialization parameters for 9600-Series SIP phones. For more information, refer to the Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones. The Avaya Administrator's Guide (ID: 160601944) contains detailed information about initializing switch parameters for 9600 SIP phones.

To create a station definition for subscriber telephones:

1 At the ASA terminal, create a station definition for each subscriber extension as shown in the following examples. Make the MWI LAMP Ext number the same as the station's extension number, and set the Coverage Path to the one you created earlier. In this example, the Coverage Path is 57.

```
display station 4021                                          Page   1 of   6
                                    STATION

Extension:    4021                    Lock Messages?   n              BCC: 0
     Type:  9620SIP                   Security Code:                  TN: 1
     Port:  S00015                  Coverage Path 1:   57            COR: 1
     Name: 4021SIP, stn4021         Coverage Path 2:                 COS: 1
                                    Hunt-to Station:
STATION OPTIONS
                                       Time of Day Lock Table:
              Loss Group:   19
                                            Message Lamp Ext:   4021

        Display Language:    english

          Survivable COR:    internal
   Survivable Trunk Dest?    y                        IP SoftPhone?   n

                                                          IP Video?  n
```

2 Associate the station with the SIP trunk that connects Session Manager. This is required for MWI purposes.

```
                                                              Page   6 of   6
                                    STATION
SIP FEATURE OPTIONS

          Type of 3PCC Enabled:   None
                      SIP Trunk:  tg57
```

3 Add the station to the off-pbx-telephone station mapping on the AAR form. AAR is used for routing of 4014.

Page 1 of 3

STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
4010	OPS	-		4010	aar	1	
4011	OPS	-		4011	aar	1	
4012	OPS	-		4012	aar	1	
4013	OPS	-		4013	aar	1	
4014	OPS	-		4014	aar	1	
4015	OPS	-		4015	aar	1	
4016	OPS	-		4016	aar	1	
4017	OPS	-		4017	aar	1	
4019	OPS	-		4019	aar	1	
4020	OPS	-		4020	aar	1	
4021	OPS	-		4021	aar	1	
5001	OPS	-		5001	tg99	1	
5002	OPS	-		5002	tg99	1	
5003	OPS	-		5003	tg99	1	

4 Add the extension number into the public-unknown-numbering form.

Page 1 of 2

NUMBERING - PUBLIC/UNKNOWN FORMAT

Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len
4	4			4
5	4	27		4
4	5	1		4
6	8		88	8
7	8	11	555	10
4	4400	11	425111	10
4	5700	57		4
4	5800	58		4

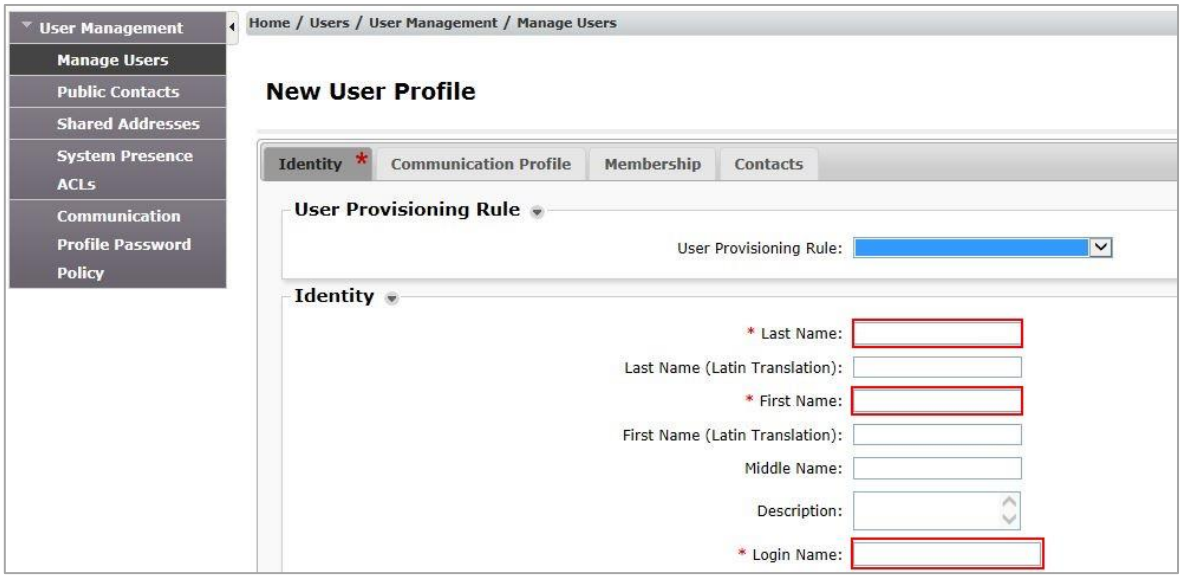
Total Administered: 8
Maximum Entries: 9999

Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.

Communication Manager automatically inserts a '+' digit in this case.

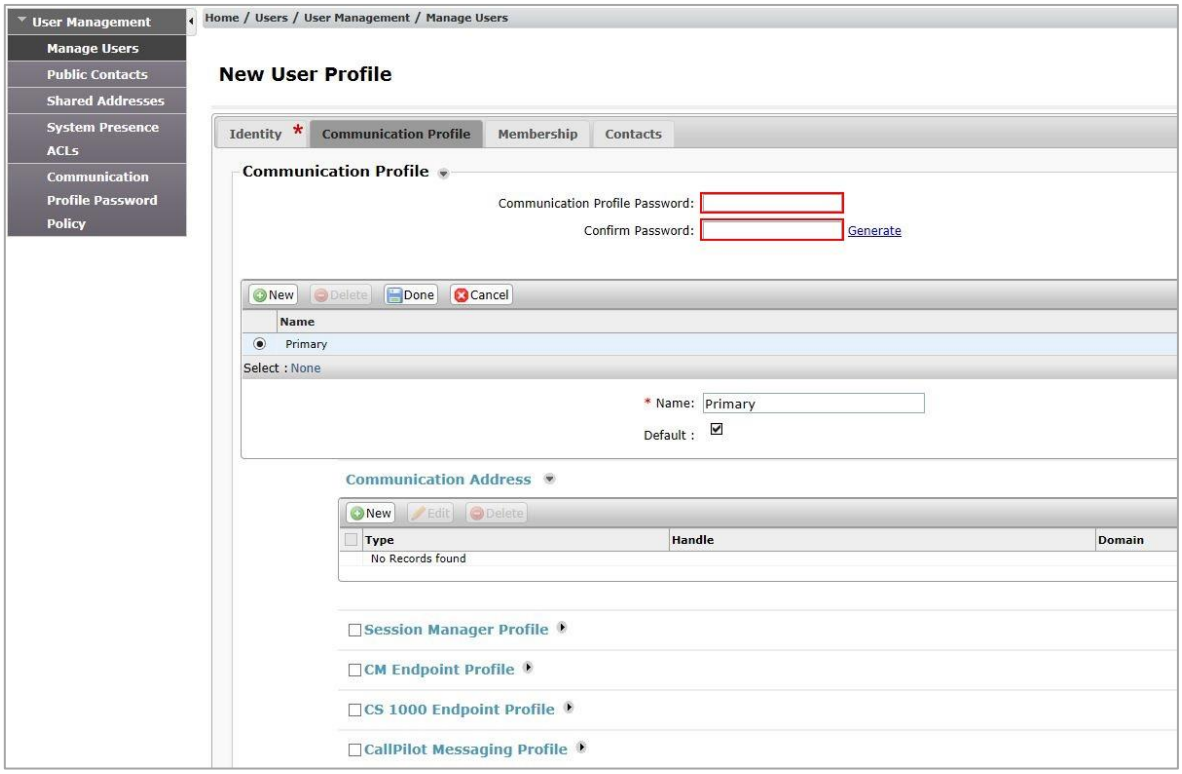
5 Log in to the System Manager, and go to **Users** > **User Management** > **Manage Users.**

6 On the **User Management** page, in the **Users** table, click **New.** The **New User Profile** page displays in the **Identity** tab.



7 In the **Identity** section, fill in the appropriate fields.

8 Click the **Communication Profile** tab.



9 In the **Communication Profile** section, add password as required.

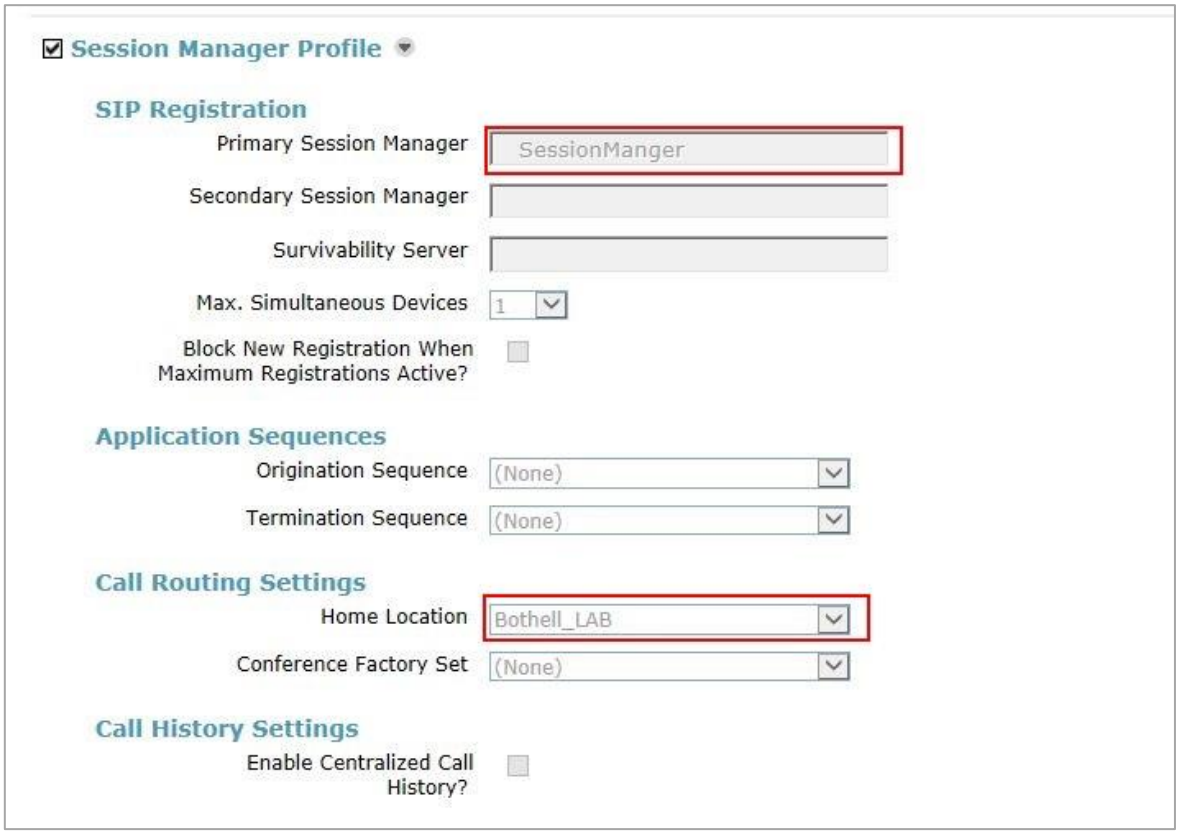
10 In the **Communication Address** section, click **New**. The options for adding a new communication address appear.

11 From the **Type** drop-down menu, select **Avaya SIP.**

12 Fill in appropriate address in the **Fully Qualified Address** fields, and then click **Add**.

13 Repeat **Steps 10** to **12** to add **Avaya E.164**.

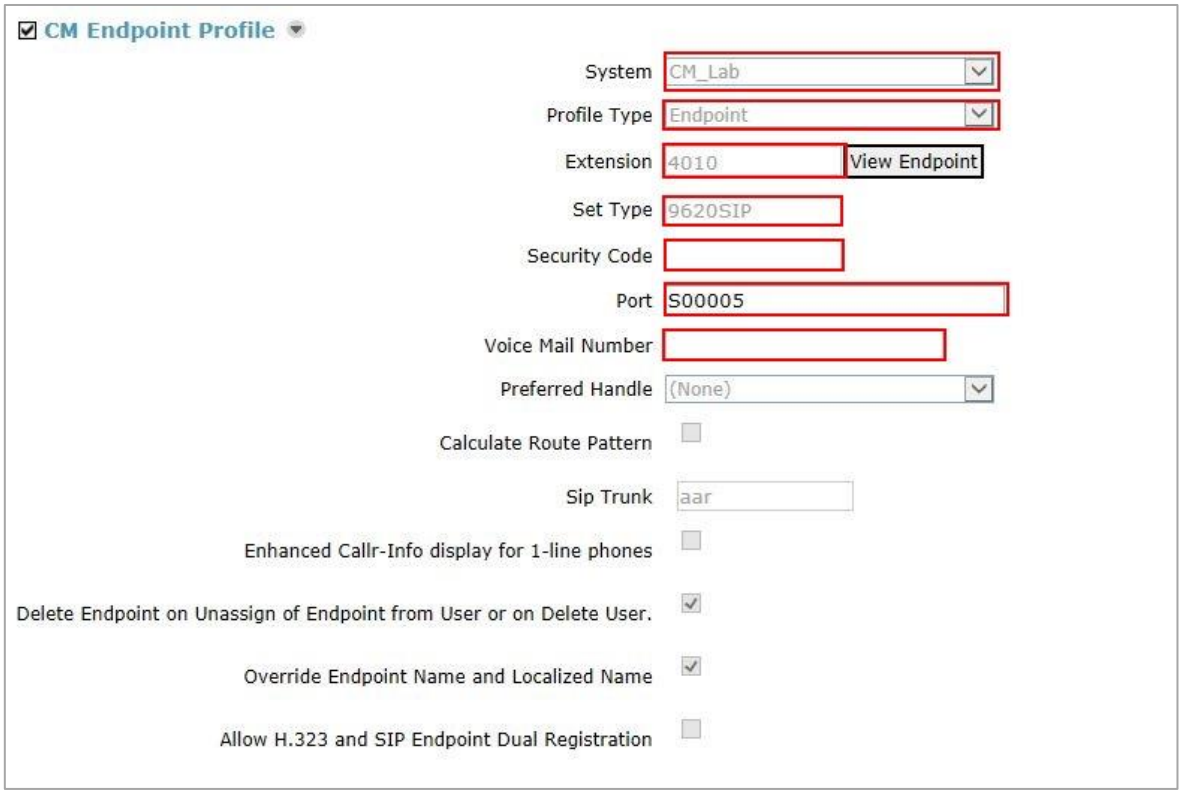
14 In the **Session Manager Profile** section, select the arrow to open the section.



15 In the **Session Manager Profile** section, fill in the following options:

- **a** In the **Primary Session Manger** field, enter or select **Session Manager**.
- **b** In the **Application Sequences** section, for the **Origination Sequence** and **Termination Sequence** options, select **CM Features**.
- **c** In the **Call Routing Settings** section, for the **Home Location** option, select the appropriate location.

16 Select the arrow icon at the end of the **CM Endpoint Profile** option to open the section.



17 In the **CM Endpoint Profile** section, fill in the appropriate options for **System**, **Profile Type**, **Extension**, **Template**, **Security Code**, **Port**, and **Voice Mail Number**.

Verifying the Local Survivable Processor settings of Telephone System

To identify the available survivable processors associated with the Avaya Communication Manager:

1 Using the System Manager, go to **Elements** > **Communication Manager** > **Element Cut-Through** or a SAT terminal connection, and then type the following command: **List Survivable-processor**. If none are listed, you do not have a secondary system that will failover and can ignore this section.

```
                              SURVIVABLE PROCESSORS
Record  Name/              Type        Reg  Act        Translations      Net
Number  IP Address                                     Updated           Rgn

 1      AVAYACMSRV         LSP         y    n          22:00 8/21/2017   2
         172.16.20.122
        No V6 Entry

 2      CM-SimplexESS2     ESS S       y    n          22:00 8/21/2017   1
         172.16.20.150
        No V6 Entry
```

2 Write down the **Record Name** and **IP Address** of the Survivable Processors listed here. You will need them later in the Configuring MiCollab AM for SIP Failover section.

3 You can also verify the screens associated with the Network Regions used for Fail-over within the Avaya Aura Communication Manager.

Display IP-Network-Map (this will show the range of IP addresses associated with each network region excluding the primary region [1])

```
display ip-network-map                                        Page   1 of   63
                              IP ADDRESS MAPPING

                                                  Subnet  Network      Emergency
IP Address                                         Bits   Region VLAN Location Ext
------------------------------------------ ------ ------ ---- -------------
FROM: 172.16.20.121                               /        2       n
  TO: 172.16.20.130
FROM:                                             /                n
  TO:
FROM:                                             /                n
  TO:
FROM:                                             /                n
  TO:
FROM:                                             /                n
  TO:
```

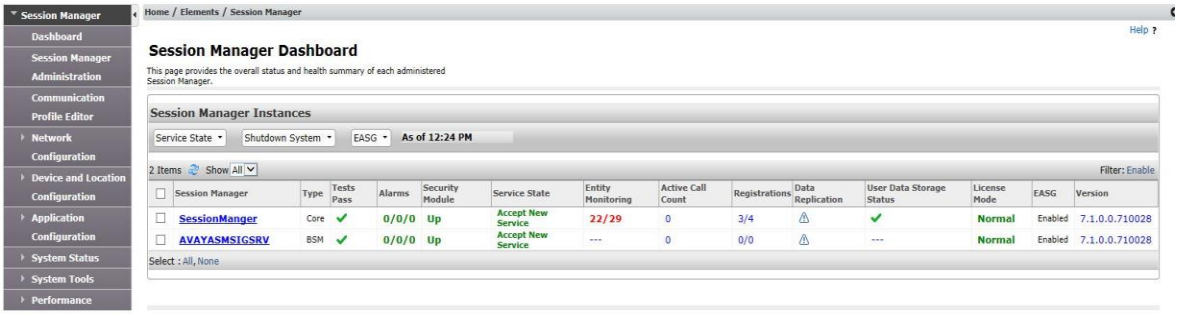
Display IP-Network-Region 2 (this will show the settings of the network region associated with each Survivable Processor)

```
display ip-network-region 2                                   Page   1 of  20
                              IP NETWORK REGION
  Region:  2        NR Group:  2
Location:  1        Authoritative Domain:     blvu.avstlabs.local
    Name: LSP                     Stub Network Region:     n
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio:        yes
      Codec Set:  1               Inter-region IP-IP Direct Audio:        yes
   UDP Port Min:  2048                      IP Audio Hairpinning?         y
   UDP Port Max:  3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value:     46
        Audio PHB Value:     46
        Video PHB Value:     26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority:       6
        Audio 802.1p Priority:       6
        Video 802.1p Priority:       5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled?   n
  H.323 Link Bounce Recovery?     y
 Idle Traffic Interval (sec):     20
   Keep-Alive Interval (sec):     5
             Keep-Alive Count:    5
```

Keep in mind that there are multiple pages of configuration settings for each Network Region.

4 On the Avaya Aura System Manager there also are a few screens that should be verified.

From the **Home** screen, Select the **Session Manager** from the **Elements** Menu. A screen similar to the following will be displayed, showing the primary server and any Survivable servers.



NOTE Security module will only show the BSM up when the failover server is running.

5 Select the **Session Manager Administration** tab to display the Instances and their individual settings.

Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

Global Settings

Save

Allow Unauthenticated Emergency Calls	☐	Disable Loop Detection Alarms	☐
Allow Unsecured PPM Traffic	☑	*Loop Detection Alarms Threshold (hours)	24
Failback Policy	Auto	Enable TLS Endpoint Certificate Validation	☐
ELIN SIP Entity	None	Enable Dial Plan Ranges	☐
Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location	☐	Enable Implicit Users Applications for SIP users	☐
Ignore SDP for Call Admission Control	☐	Enable End to End Secure Call Indication	☐
Disable Call Admission Control Threshold Alarms	☐		

Session Manager Instances

New View Edit Delete

1 Item Filter: Enable

	Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
○	SessionManger	Normal	57	0	57	AVST Lab

Select : None

Branch Session Manager Instances

New View Edit Delete

1 Item Filter: Enable

	Name	License Mode	Main CM for LSP	SIP Communication Profiles	Description
○	AVAYASMSIGSRV	Normal	CM_Lab	0	

Select : None

NOTE For additional information, please refer to the Avaya Aura documentation for System Manager and Session Manager.

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 exiting MiCollab AM system.

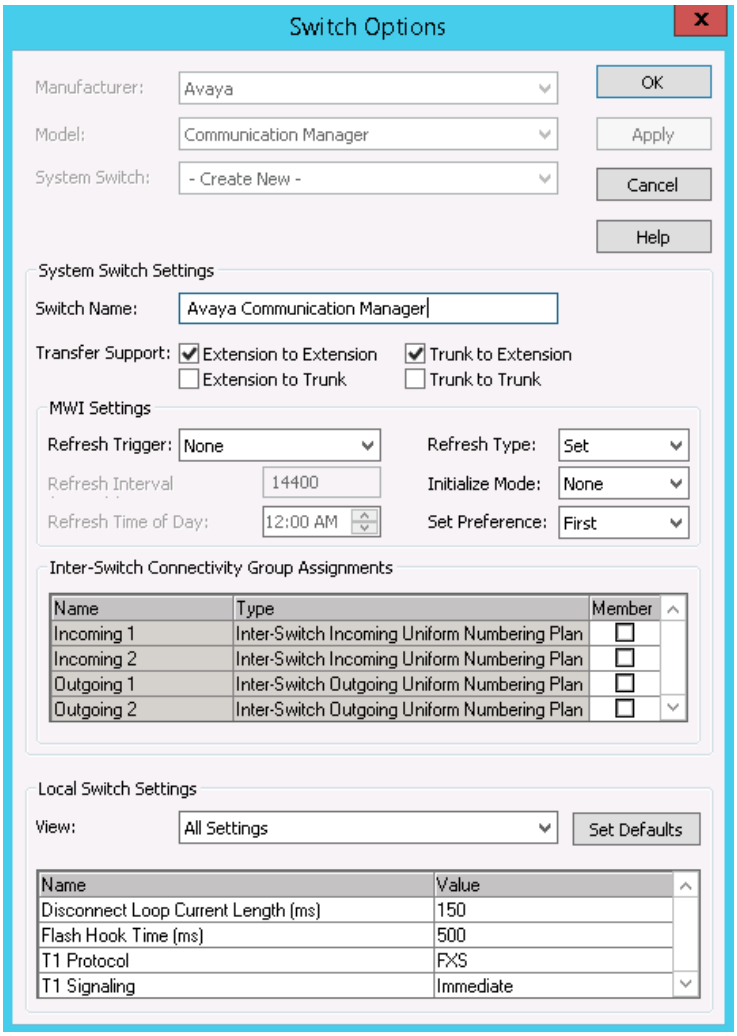
NOTE For general information on integrations, refer to the **Integrating MiCollab AM with the Telephone System** chapter in the *System Installation and Configuration Guide*, and the topic, **Integrating MiCollab AM with the Telephone System**, in the online help.

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** drop-down list, select **Avaya**.
   - **d** From the **Model** drop-down list, select **Communication Manager**.
   - **e** From the **Integration Type** drop-down list, select **SIP Trunk**.
2. Click **Next**. 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**.

3 Click **OK**. The **Switch Options** dialog box appears.

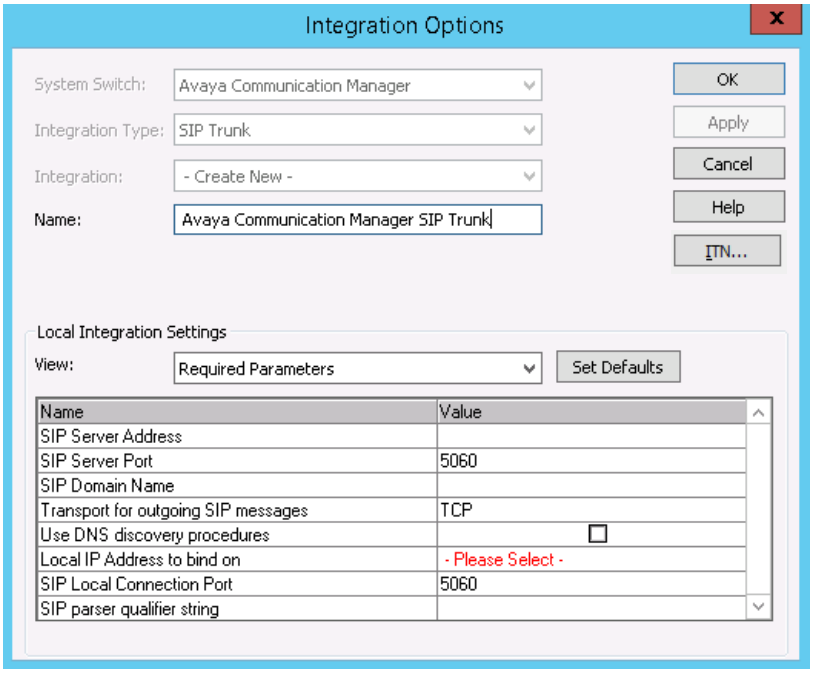


4 If necessary, make any changes to the default settings your site requires in the **Switch Options** dialog box.

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*.

5 Click **OK**. The **Integration Options** dialog box appears.



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

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

Table 4. Required Parameters View – Integration Options

Field	Required Value
SIP Server Address	**For the SIP trunk with SM integrations:** Enter the IP address of the Session Manager server. **For the Direct SIP trunk integrations.** Enter the IP address of the CM procr.
SIP Server Port	Enter the port number on which the Session Manager or CM listens for SIP messages. For the SM, this port **must** match the Session Manager port configured as an Entity Link for MiCollab AM. The default port number is 5060.
SIP Domain Name	Enter the SIP domain name. This value must be the same value as defined as am IP interface. **IMPORTANT** Be sure the Authoritative Domain name is the same throughout the Session Manager server, Communication Manager, and MiCollab AM programming.
Transport for outgoing SIP messages	Enter **TCP** or **UDP** (**TCP** is the default value.) **NOTE** This value must match the protocol selected on the Entity Link created for MiCollab AM Call Server.

Use DNS discovery procedures	Select this box to use DNS discovery.
Local IP Address to bind on	Enter the IP address of the network interface card (NIC) on the Call Server platform that supports the SIP integration. If there is only one NIC on the MiCollab AM server platform, this field typically contains the IP address of that NIC already.
SIP Location Connection Port	Enter the port number on which MiCollab AM listens for incoming SIP messages. The default value is **5060**.
Sip parser qualifier string	*In cases of a 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. In cases where there are multiple SIP integrations on the call server, use a string that is unique to each SIP integration. **For example:** 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. 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 following option:

- Set the **Type of Call Progress to use for External Calls** value. How this should be set depends on the gateway used for the integration as follows:
  - **Digital**: Select Digital if the gateway supports call progress through to the endpoint.
  - **Media**: Select Media if the gateway reports early that the call is connected, such as before the phone rings or while the phone is ringing.

c In the **Local Integration Settings** section, select the **Media Settings** view and configure the following option:

- Select the checkbox in the **Validate Remote Hosts for Media**, if you want to use this feature.

IMPORTANT Enabling this parameter causes processing overhead and should only be enabled when necessary. For information on this setting, see the note in the section, Critical Application Considerations.

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

7 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 the **Incoming Hunt Mode** field, select the mode for this integration.

c In the **Hunt Group Access Code** box, type the hunt pilot number you defined earlier in the Creating a Hunt Group and Pilot Number section. This is the pilot number that users dial to reach MiCollab AM.

d Click **OK**.

8 Continue through and complete the configuration. At the end of the configuration, a confirmation dialog box appears. Click **OK**.

9 If **MiCollab AM Configuration** does not open automatically after the configuration completes, open **MiCollab AM Configuration**, and select the **Lines** tab.

10 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.

11 Click **OK** to save all changes.

Configuring Existing MiCollab AM for the Integration

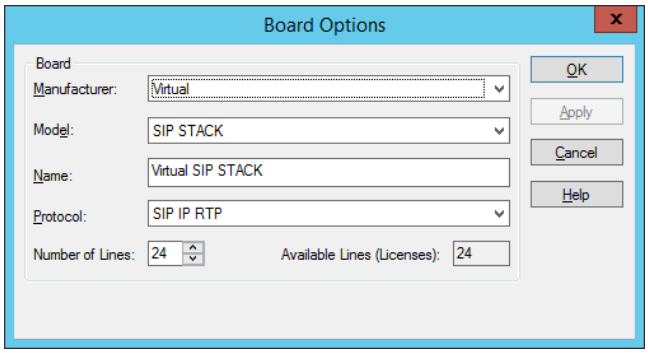
To configure exiting MiCollab AM for the telephone integration:

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**.

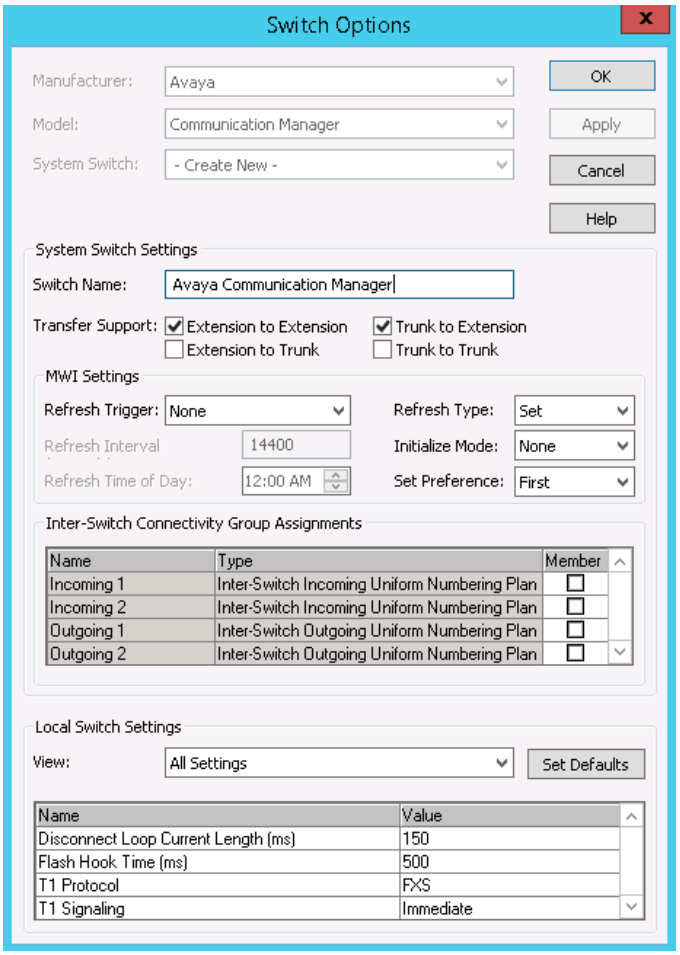
4 Select the **Switches** tab and click the **Add** button. The **Switch Integration Data Setup** dialog box appears.

a From the **Manufacturer** drop-down list, select **Avaya**.

b From the **Model** drop-down list, select **Communication Manager**.

c From the **Integration Type** drop-down list, select **SIP Trunk**.

5 Click **OK**. The **Switch Options** dialog box appears.

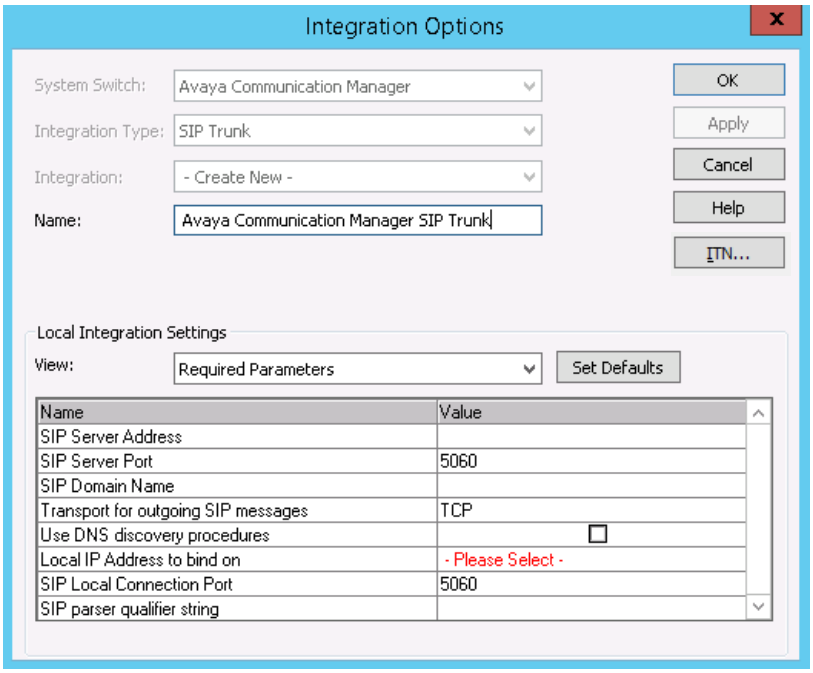


6 If necessary, make any changes to the default settings your site requires in the **Switch Options** dialog box.

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.



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

a In the **Local Integration Options** 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	**For the SIP trunk with SM integrations:** Enter the IP address of the Session Manager server. **For the Direct SIP trunk integrations.** Enter the IP address of the CM procr.
SIP Server Port	Enter the port number on which the Session Manager or CM listens for SIP messages. For the SM, this port **must** match the Session Manager port configured as an Entity Link for MiCollab AM. The default port number is 5060.
SIP Domain Name	Enter the SIP domain name. This value must be the same value as defined as am IP interface. **IMPORTANT** Be sure the Authoritative Domain name is the same throughout the Session Manager server, Communication Manager, and MiCollab AM programming.
Transport for outgoing SIP messages	Enter **TCP** or **UDP** (**TCP** is the default value.) **NOTE** This value must match the protocol selected on the Entity Link created for MiCollab AM Call Server.

Use DNS discovery procedures	Select this box to use DNS discovery.
Local IP Address to bind on	Enter the IP address of the network interface card (NIC) on the Call Server platform that supports the SIP integration. If there is only one NIC on the MiCollab AM server platform, this field typically contains the IP address of that NIC already.
SIP Location Connection Port	Enter the port number on which MiCollab AM listens for incoming SIP messages. The default value is **5060**.
Sip parser qualifier string	*In cases of a 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. In cases where there are multiple SIP integrations on the call server, use a string that is unique to each SIP integration. **For example:** 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. 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 following option:

- Set the **Type of Call Progress to use for External Calls** value. How this should be set depends on the gateway used for the integration as follows:
  - **Digital**: Select Digital if the gateway supports call progress through to the endpoint.
  - **Media**: Select Media if the gateway reports early that the call is connected, such as before the phone rings or while the phone is ringing.

c In the **Local Integration Settings** section, select the **Media Settings** view and configure the following option:

- Select the checkbox in the **Validate Remote Hosts for Media**, if you want to use this feature.

IMPORTANT Enabling this parameter causes processing overhead and should only be enabled when necessary. For information on this setting, see the note in the section, Critical Application Considerations.

d 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 Switch Section Settings** section, select the **Required Parameters** view.

b In the **Incoming Hunt Mode** field, select the mode for this integration.

c In the **Hunt Group Access Code** box, type the hunt pilot number you defined earlier in the Creating a Hunt Group and Pilot Number section. This is the pilot number that users dial to reach MiCollab AM.

d Click **OK**.

10 In **MiCollab AM Configuration**, verify that that the telephone system is properly added and configured in the **Switches**, **Switch Sections**, and **Integrations** tabs.

11 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 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:

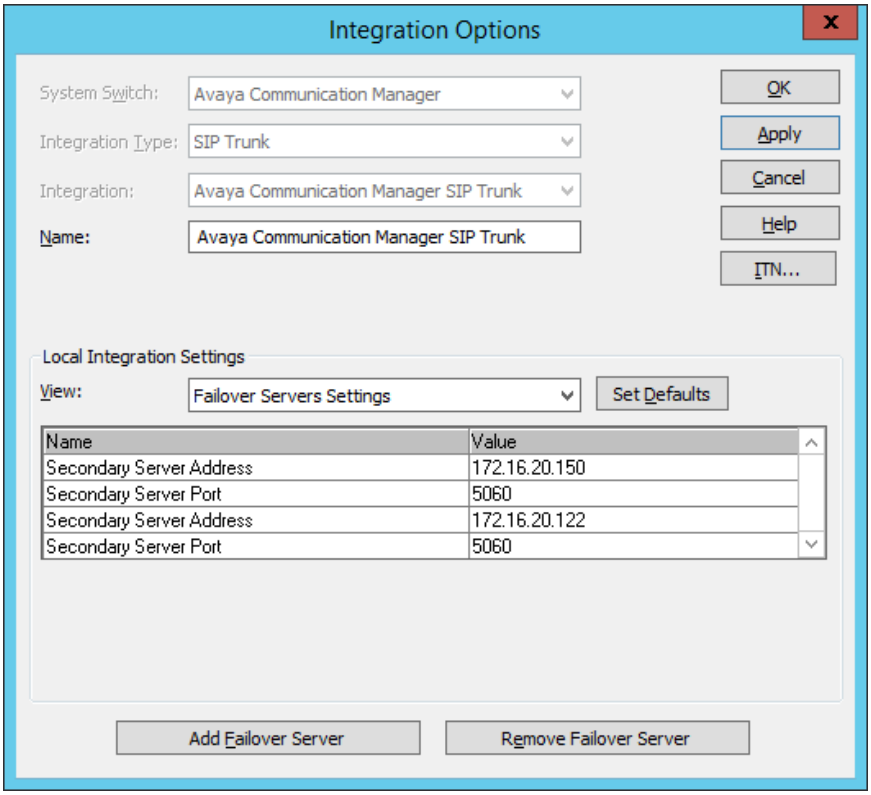
Table 6. Secondary SIP Server Address and the Secondary SIP Server Port example

Field	Value
Secondary SIP Server Address	Enter the TCP/IP address or an FQDN of the secondary node. **For example:** The IP address for a Survivable Remote Server (formerly LSP) is 172.16.20.122 as displayed on the Review/Modify SIP Gateway screen. The IP address for a Survivable Core Server (formerly ESS) is 172.16.20.150 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 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	How this should be set depends on the gateway used for the integration. • 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.

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**.
1. In the **Control Panel**, click **Network and Internet** > **Network and Sharing Center**.
2. On the left pane, select **Change Adapter Settings**.
3. Press Alt to display the menu bar.
4. On the menu bar, select **Advanced**, and then click **Advanced Settings**.
5. On the **Adapters and Bindings** tab of **Advanced Settings**, click the network connection that serves MiCollab AM.
6. 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.
7. 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 8. QoS Configuration

Field	Setting
Application Name	At_TelephonyServer.exe
Protocol	Match the setting used for the integration UDP or TCP
Source Port	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: BasePortNumber + (NumberOfCXPorts * 10) -1. Hence, if the base port is 10000, and MiCollab AM has 8 lines, then the port range to use would be: 10000:10079
DSCP Value	46