MiCollab Advanced Messaging

Avaya Communication Manager SRTP/TLS SIP Station with Session Manager

Integration Technical Note

For version 9.1 and above

1082-10430-8784
Rev 9.1.0.5.2 October 2020

Notice

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

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

Trademarks

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

© Copyright 2020, Mitel Networks Corporation

All rights reserved

Contents

Preface 5

References 6

Documentation 6

Documentation Updates 6

Help 7

Document Conventions 7

Features Supported by This Integration 8

Critical Application Considerations 11

Installation Requirements 16

Telephone System Requirements 16

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 19

Creating a SIP Trunk Group 20

Configuring Aura System Manager 23

Configuring Domain 23

Configuring Locations 24

Configuring Adaptation 25

Configuring SIP Entities 26

Configuring Entity Links 28

Configuring Time Ranges 29

Configuring Routing Policies 29

Adding Avaya Trusted Certificates 31

Adding Trusted Certificates 31

Setting up Avaya SRTP SIP 33

Programming MiCollab AM Ports 34

Configuring the SIP Entities on Avaya Servers 36
Configuring the Session Manager Firewall 39
Configuring the Routing Policies 41
Adding the MiCollab AM Port User Definitions 42
Creating a Hunt Group and Pilot Number 44
Creating a Coverage Path 45
Creating a Route Pattern 46
Modifying Digit Conversion Tables 47
Defining the Telephone System Location 48
Programming Subscriber Telephones 48

Configuring MiCollab AM 55

Configuring MiCollab AM for the Integration During Initial Installation 55
Configuring Existing MiCollab AM for the Integration 60
Configuring MiCollab AM for SIP Failover 65

Changing the Network Binding Order on the MiCollab AM Platform 68

Windows Server 2012 R2 68
Windows Server 2016 / 2019 69

Configuring Quality of Service (QoS) 70

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.

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 five major components:

- The Avaya Aura Communication Manager
- The Avaya G430/G450/G650 Media Gateway
- Avaya Aura Session Manager server
- Avaya Aura System Manager server
- MiCollab AM

MiCollab AM registers its SIP ports as terminals or endpoints with the Avaya Aura Session Manager server. The SIP ports are configured as Off-Premises Stations (OPS) and are assigned into a hunt group of the PBX.

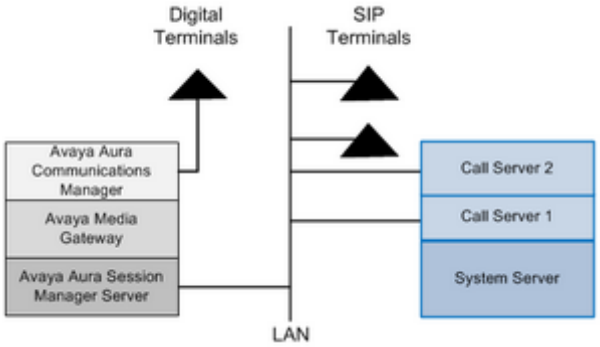


Figure 1. Avaya Communication Manager SIP Integration

Calls intended for MiCollab AM, whether direct or forwarded, are directed to the pilot number of this hunt group. The Call Server uses these same lines to place or transfer calls to the telephone system.

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.

The integration process consists of configuring SIP support on the media server, configuring the telephone system at the gateway, configuring subscriber workstations at the media server, 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.

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 SRTP-TLS SIP Station 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 Communication Manager SRTP/TLS SIP Station

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 1, 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	Yes	Note 3
TLS	Yes	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 next section, Critical Application Considerations.
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 populate Line extension numbers on the **Lines** tab before starting MiCollab AM or the integration will fail. The extension numbers are registered as SIP stations with the IP PBX during system startup.
- Configure the MiCollab AM **Incoming Hunt Mode** in the **Switch Section Options** dialog box. The hunt mode must match the type of hunting provided by the IP PBX. This helps to alleviate any "glare" conditions between the IP PBX and the Call Server. The default mode is Terminal.
- You must configure the **Hunt Group Access Code** in the **Switch Section Options** dialog box. This code cannot conflict with extensions.

  > **For example:**
  >
  > You can use 6000 for the Hunt Group Access Code and start MiCollab AM extensions with 6001.

- On a MiCollab AM server with two or more NICs, the NIC that supports this integration must not occupy first place in the operating system's binding order. The primary (public) network interface card (NIC) must be the first network connection in the network binding order. MiCollab AM binds and communicates to other servers and subscribers on this network connection. For more information, refer to Changing the Network Binding Order on the MiCollab AM Platform.
- MiCollab AM supports G.729a with support for annex b on the incoming audio stream only. MiCollab AM does not transmit annex b packets.
- When codec negotiation takes place between MiCollab AM and the PBX, MiCollab AM always offers the G.729a audio format as an option. You may configure G.729a as the preferred codec in MiCollab AM; however, the decision whether to use G.729a is always made by the PBX.
- The 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 an environment with Avaya Communication Manager, Session Manager, Avaya/Nortel CS1000 Call server and Signaling Server, there are limitations in transferring to Avaya/Nortel phones registered to the Signaling Server.
- If another application requiring a different configuration 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 7.0 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 9.1 supports up to 10 integration types (i.e., licensed integrations) in total per system. However, the following limitations apply to each Call Server:
  - Limited to 3 integration types per Call Server
  - The 3 integration types can be any mix of TDM and SIP (e.g., 1 TDM and 2 SIP)
  - Limited to 1 Cisco UCM SCCP IP integration. Can be mixed with TDM, but not with SIP
  - Connect up to 10 telephone systems total per Call Server (e.g., 2 Avaya Communication Manager systems using SIP + 5 Avaya IP Office systems using SIP + 3 Siemens HiPath 4000 systems using Station Set Emulation)
  - SIP timers for Aastra EETS integrations are incompatible with other SIP integrations. Thus, it is not possible to have an EETS integration with any other SIP integration on the Call Server.

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

Installation Requirements

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

Telephone System Requirements

- Avaya Aura Communication Manager 8.1 and prior
- Avaya Aura Session Manager 8.1 and prior
- Avaya Aura G430 or G450 Media Gateways with possible additional DSP resources required; or G650 with C-LAN and IP Media Processor with current firmware update, to handle voice processing tasks
- TN2302/TN2602 IP Media Processor with current firmware update, to handle voice processing tasks (Applicable only in G650 configuration)
- TN799D C-LAN to process signaling information (Applicable only in G650 configuration)
- One Off-Premises Station (OPS) license per MiCollab AM port
- One Administered SIP Trunk license per MiCollab AM port
- 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 9.1
- MiCollab AM software key diskette or feature file with the Avaya Communication Manager SIP trunk 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

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 and OPS Extension 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.

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 Communication Manager Element Cut-Through from Avaya System Manager or a SAT terminal, define a Signaling Group associating the Communication Manager and Session Manager servers, as shown in the following example.

To create SIP Signaling Group:

1. Specify a node name for the **Session Manager** and a listening port accessible to both the **Session Manager** and **Communication Manager** servers.
2. Specify the name of the domain on which the MiCollab AM platform is located.
3. Enable **Direct IP-to-IP Audio Connections** and **IP Audio Hairpinning**.
4. Specify the **rtp-payload** method for the telephone system to use in transmitting DTMF tone sequences over the IP network.

```
change signaling-group 1                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number:  1                 Group Type:  sip
  IMS Enabled?  n          Transport Method:  tls
        Q-SIP?  n
     IP Video?  n                                   Enforce SIPS URI for SRTP?  y
 Peer Detection Enabled?  y  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:  clan1                  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?  y
Session Establishment Timer(min):  3                 IP Audio Hairpinning?  y
         Enable Layer 3 Test?  y               Initial IP-IP Direct Media?  n
H.323 Station Outgoing Direct Media?  n        Alternate Route Timer(sec):  6
```

Defining the IP Interfaces

Define the IP Authoritative Domain and IP interfaces.

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

Figure 2. Avaya System Manager

```
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 a SIP Trunk Group

Create a Trunk Group and populate it with the ports that support the MiCollab AM integration, as shown in the following two examples.

To create a SIP Trunk Group:

1 Specify sip as the **Group Type** and tie as the **Service Type**. (Page 1)

```
                                                              Page   1 of  21
                                TRUNK GROUP

Group Number:  1                    Group Type:  sip          CDR Reports:  y
  Group Name:  sip trunk - tls          COR:  1     TN:  1     TAC:  201
   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:  1
                                       Number of Members:  255
```

2 Set the **Preferred Minimum Session Refresh Interval** to **12000**. (Page 2)

```
                                                          Page   2 of   21
        Group Type:   sip

TRUNK PARAMETERS

      Unicode Name:  yes

                                        Redirect On OPTIM Failure:   5000

            SCCAN?  n                          Digital Loss Group:   18
                     Preferred Minimum Session Refresh Interval(sec):  12000

 Disconnect Supervision -      In?  y  Out?  n

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


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

3 Verify that the settings match the following: (Page 3)

```
                                                          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
```

4 Verify that the settings match the following: (Page 4)

Page 4 of 21

PROTOCOL VARIATIONS

Mark Users as Phone?	n
Prepend '+' to Calling/Alerting/Diverting/Connected Number?	n
Send Transferring Party Information?	y
Network Call Redirection?	y
Build Refer-To URI of REFER From Contact For NCR?	n
Send Diversion Header?	n
Support Request History?	y
Telephone Event Payload Type:	101
Convert 180 to 183 for Early Media?	n
Always Use re-INVITE for Display Updates?	n
Identity for Calling Party Display:	P-Asserted-Identity
Block Sending Calling Party Location in INVITE?	n
Accept Redirect to Blank User Destination?	n
Enable Q-SIP?	n
Interworking of ISDN Clearing with In-Band Tones:	keep-channel-active
Request URI Contents:	may-have-extra-digits

5 Associate the new **Trunk Group** with the **Signaling Group** you created previously.

Page 5 of 21

TRUNK GROUP

Administered Members (min/max): 1/255

GROUP MEMBER ASSIGNMENTS Total Administered Members: 255

	Port	Name
1:	T00001	sip trunk
2:	T00002	sip trunk
3:	T00003	sip trunk
4:	T00004	sip trunk
5:	T00005	sip trunk
6:	T00006	sip trunk
7:	T00007	sip trunk
8:	T00008	sip trunk
9:	T00009	sip trunk
10:	T00010	sip trunk
11:	T00011	sip trunk
12:	T00012	sip trunk
13:	T00013	sip trunk
14:	T00014	sip trunk
15:	T00015	sip trunk

Configuring Aura System Manager

In order to use SRTP/TLS, you must properly configure routing in the Avaya Aura System Manager. The image below displays the main screen of the Avaya Aura System Manager. To configure the System Manager, follow the steps in the subsequent sections.

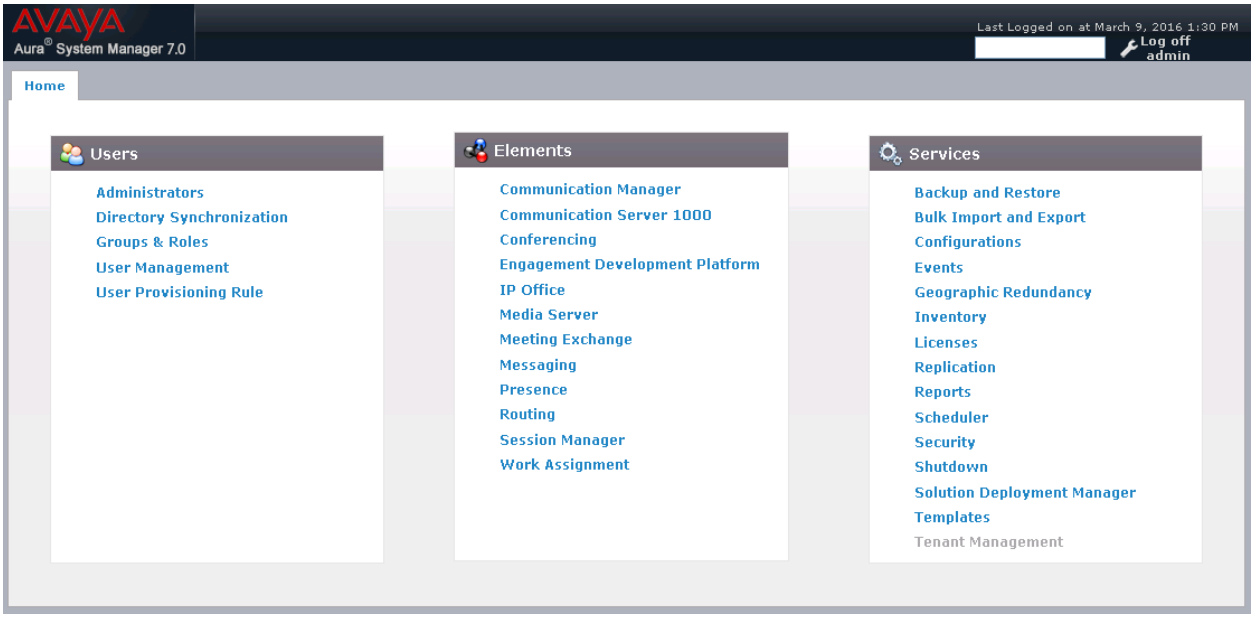


Figure 3. Avaya Aura System Manager

Configuring Domain

Log in to the System Manager, and go to **Elements** > **Routing** > **Domains**. The list of available domains appears in the **Domain Management** page.

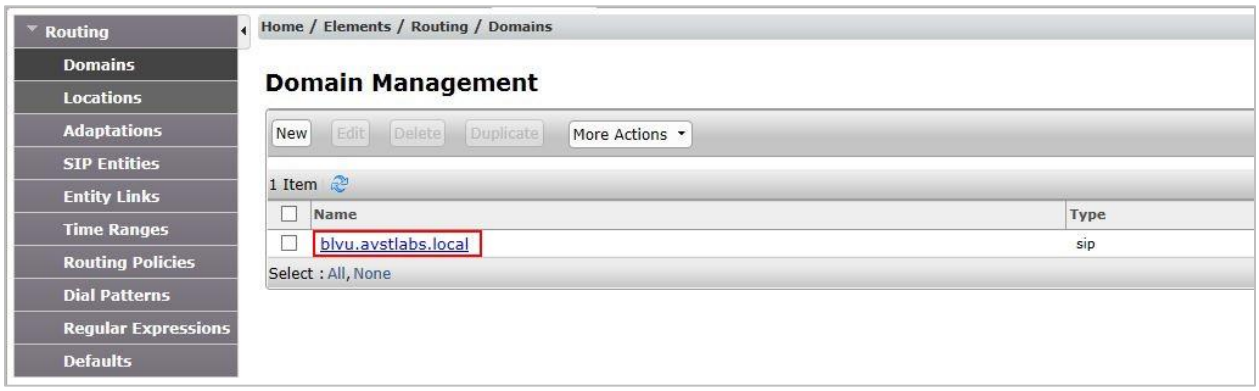
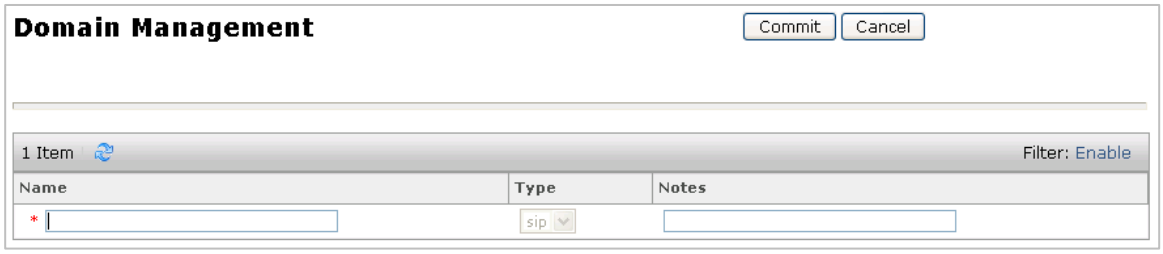


Figure 4. System Manager – Routing Domain Management

- To add a new domain, click **New**.
- To edit an existing domain, select the domain name, or select the domain checkbox and click **Edit**.
- On the **Domain Management** page, configure the required **Name** field; and the remaining fields appropriate for your organization.



Configuring Locations

Log in to the System Manager, and go to **Elements** > **Routing** > **Locations**. The list of available locations appears in the **Location** page.

Figure 5. System Manager – Routing Location

- To add a new location, click **New**.
- To edit an existing location, select the location name, or select the location checkbox and click **Edit**.
- On the **Location Details** page, configure the required **Name** field; and the remaining fields appropriate for your organization especially the **Per-Call Bandwidth Parameters** and **Alarm Threshold** sections.

Location Details Commit Cancel

General

* Name: Bothell_LAB

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Configuring Adaptation

Log in to the System Manager, and go to **Elements** > **Routing** > **Adaptations**. The list of available adaptations appears in the **Adaptations** page.

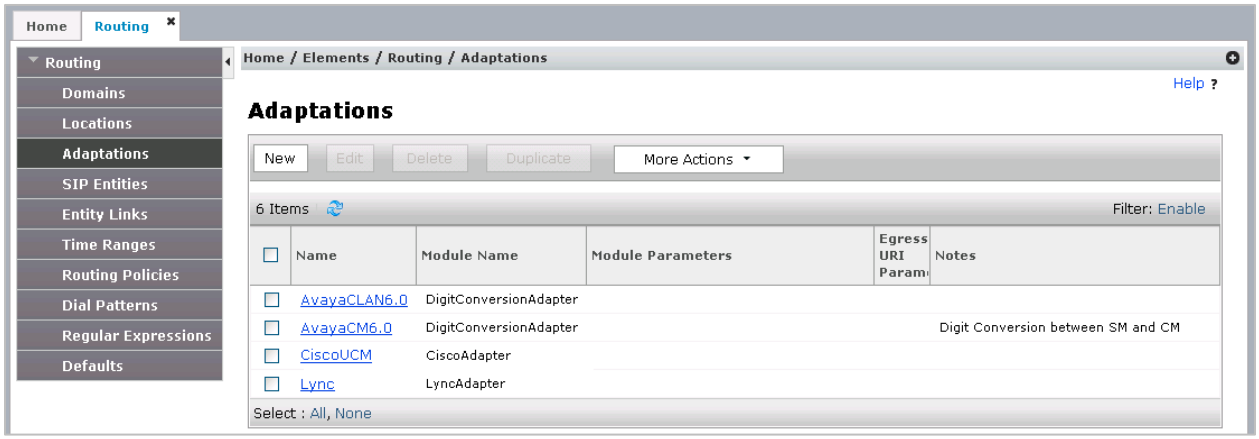
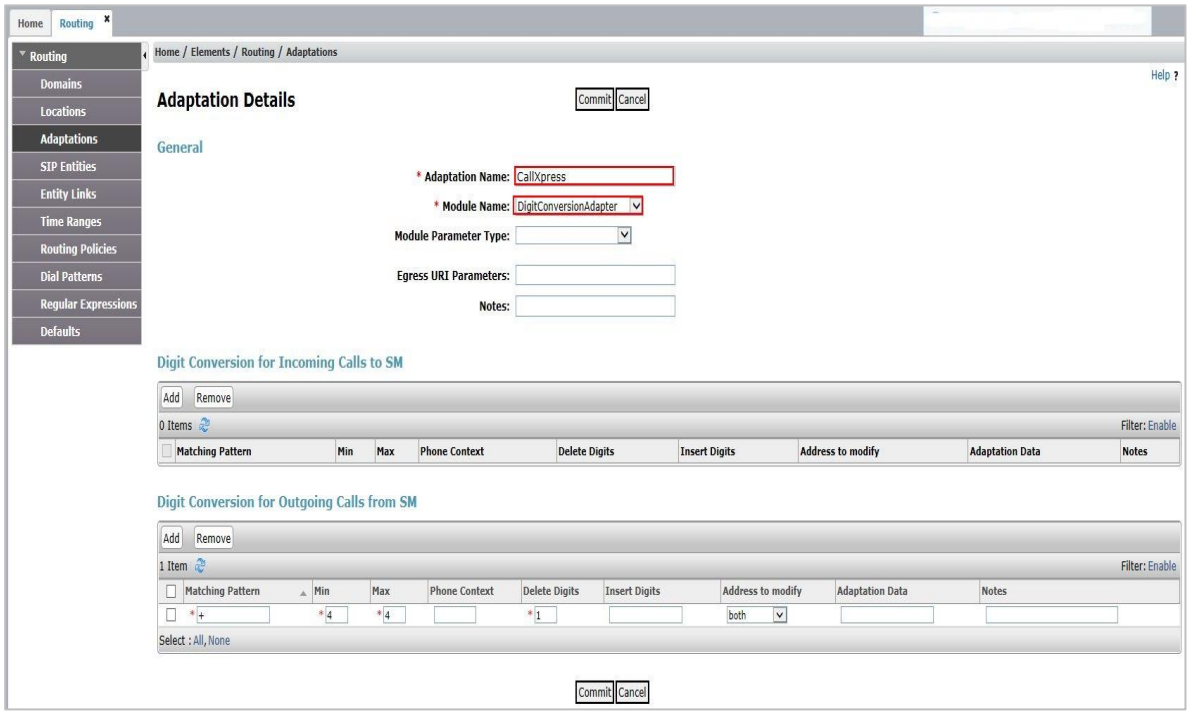


Figure 6. System Manager – Routing Adaptations

- To add a new adaptation, click **New**.
- To edit an existing adaptation, select the adaptation name, or select the adaptation checkbox and click **Edit**.
- On the **Adaptation Details** page, configure the required **Adaptation Name** and **Module Name** fields and the remaining fields appropriate for your organization.



Configuring SIP Entities

Log in to the System Manager, and go to **Elements** > **Routing** > **SIP Entities**. The list of available SIP entities appears in the **SIP Entities** page.

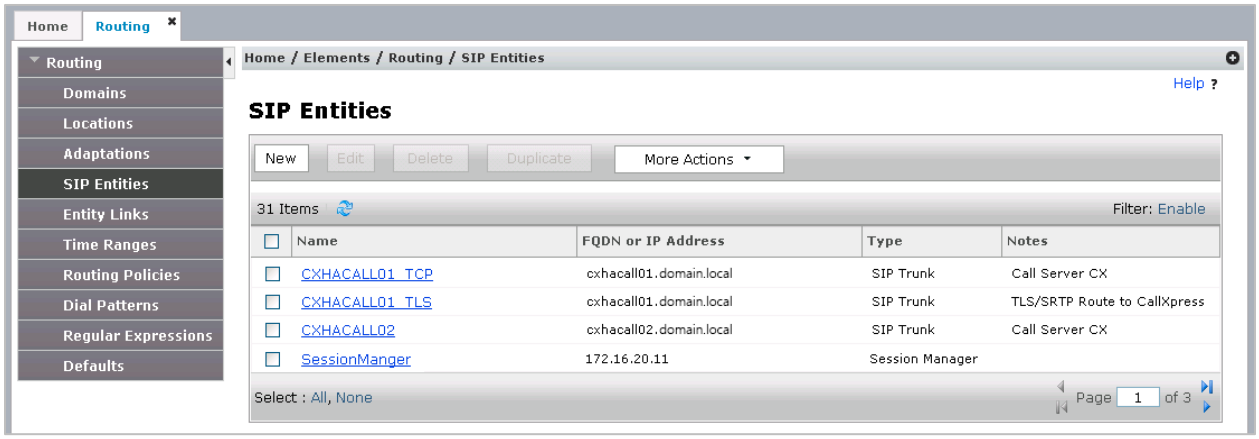
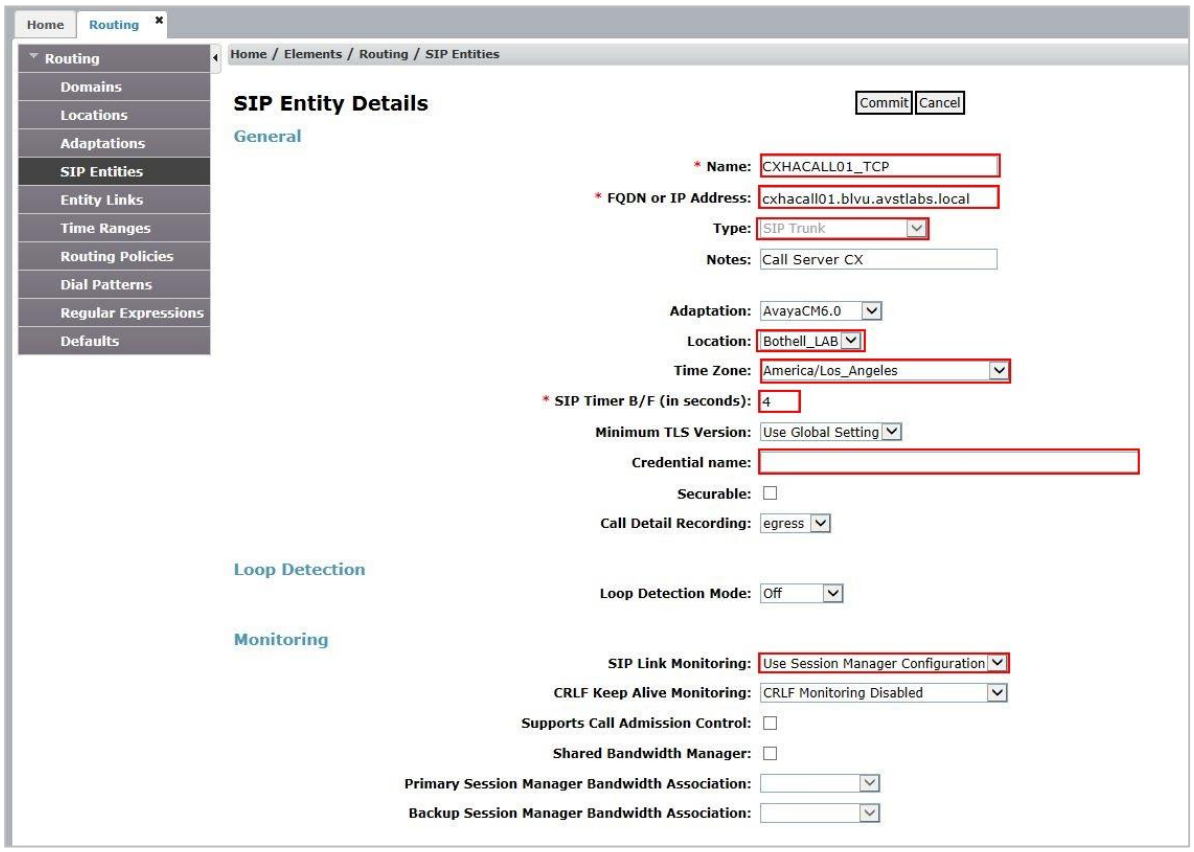
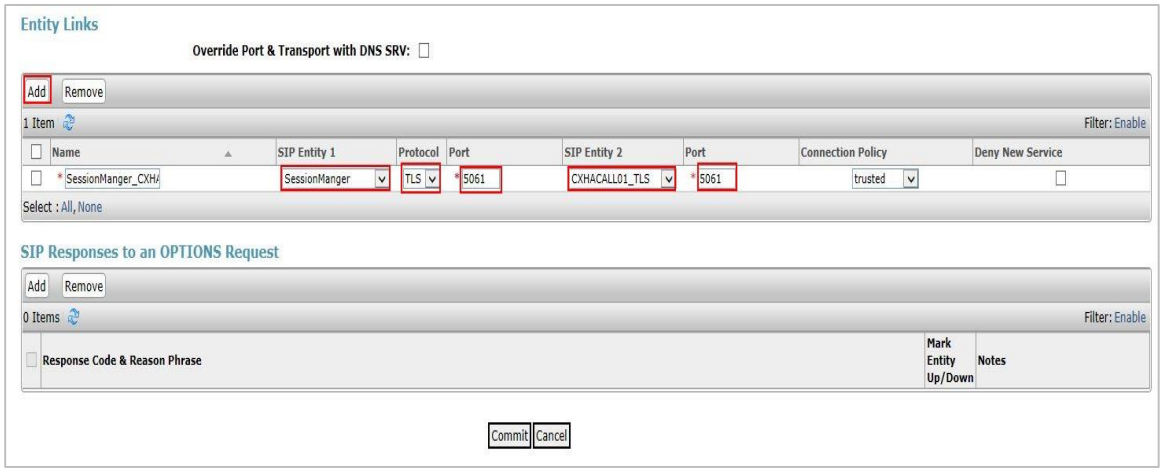


Figure 7. System Manager – Routing Location

- To add a new SIP Entity, click **New**.
- To edit an existing SIP Entity, select the SIP Entity name, or select the SIP Entity checkbox and click **Edit**.
- On the **SIP Entity Details** page, configure the required **Name** and **FQDN or IP Address** fields; and the remaining fields appropriate for your organization.





Configuring Entity Links

Log in to the System Manager, and go to **Elements** > **Routing** > **Entity Links**. The list of available entity links appears in the **Entity Links** page.

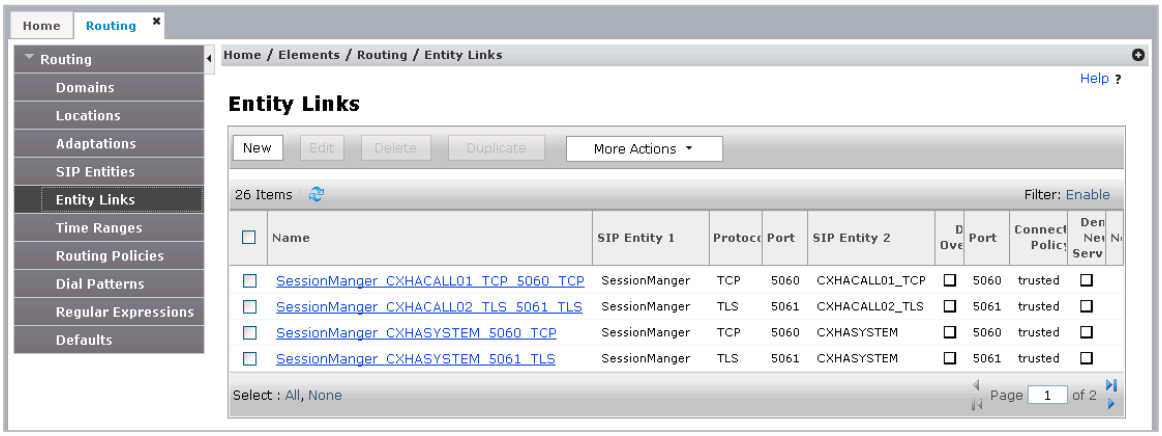
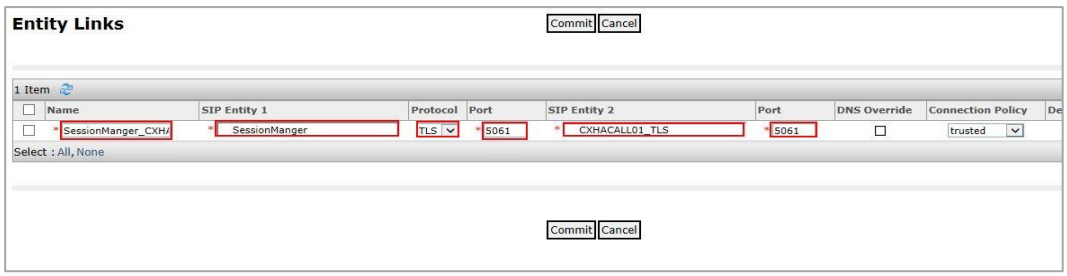


Figure 8. System Manager – Routing Entity Links

- To add a new Entity Link, click **New**.
- To edit an existing Entity Link, select the Entity Link name, or select the Entity Link checkbox and click **Edit**.
- On the **Entity Links** page, configure the required **Name**, **SIP Entity 1**, **Protocol**, **Port**, **SIP Entity 2**, and **Port** fields and the remaining fields appropriate for your organization.



Configuring Time Ranges

Log in to the System Manager, and go to **Elements** > **Routing** > **Time Ranges**. The list of available time ranges appears in the **Time Ranges** page.

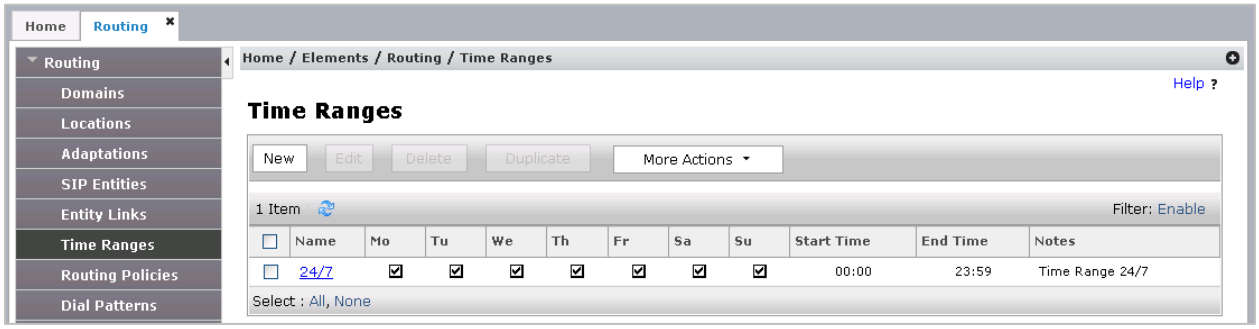
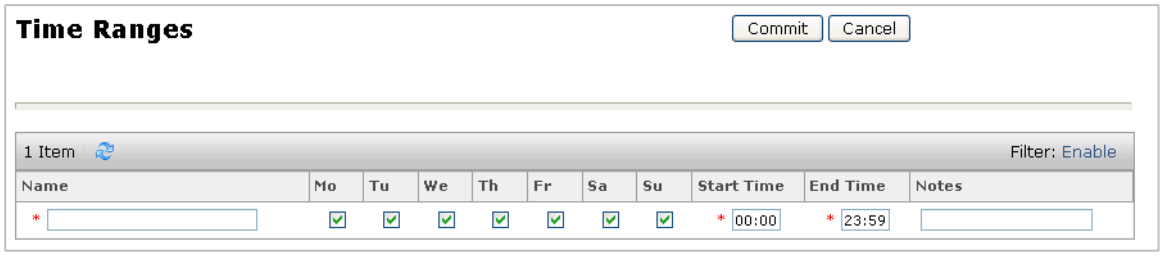


Figure 9. System Manager – Routing Time Ranges

- To add a new Time Range, click **New**.
- To edit an existing Time Range, select the Time Range name, or select the Time Range checkbox and click **Edit**.
- On the **Time Ranges** page, configure the required **Name**, **Start Time**, and **End Time** fields; and the the days of the week boxes appropriate for you organization.



Configuring Routing Policies

Log in to the System Manager, and go to **Elements** > **Routing** > **Routing Policies**. The list of available routing policies links appears in the **Routing Policies** page.

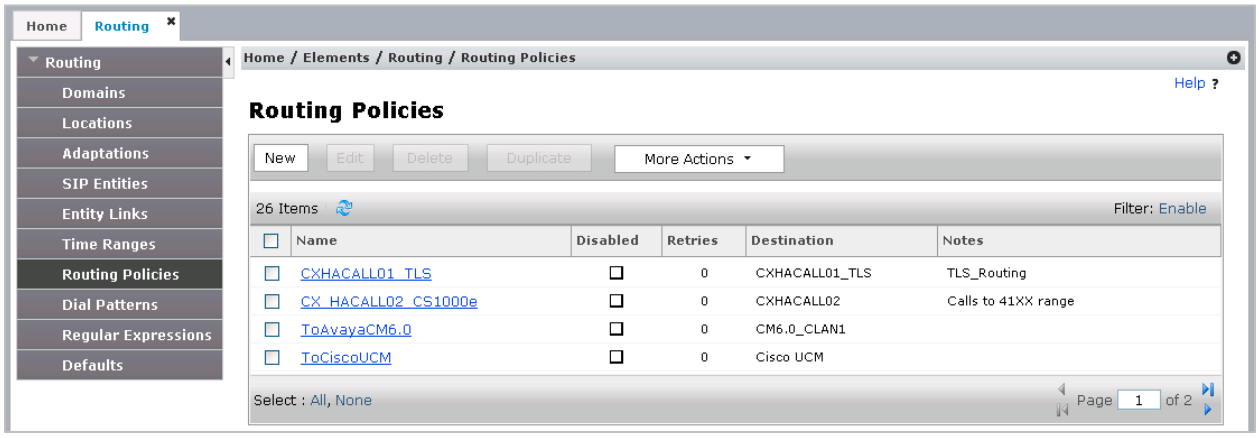
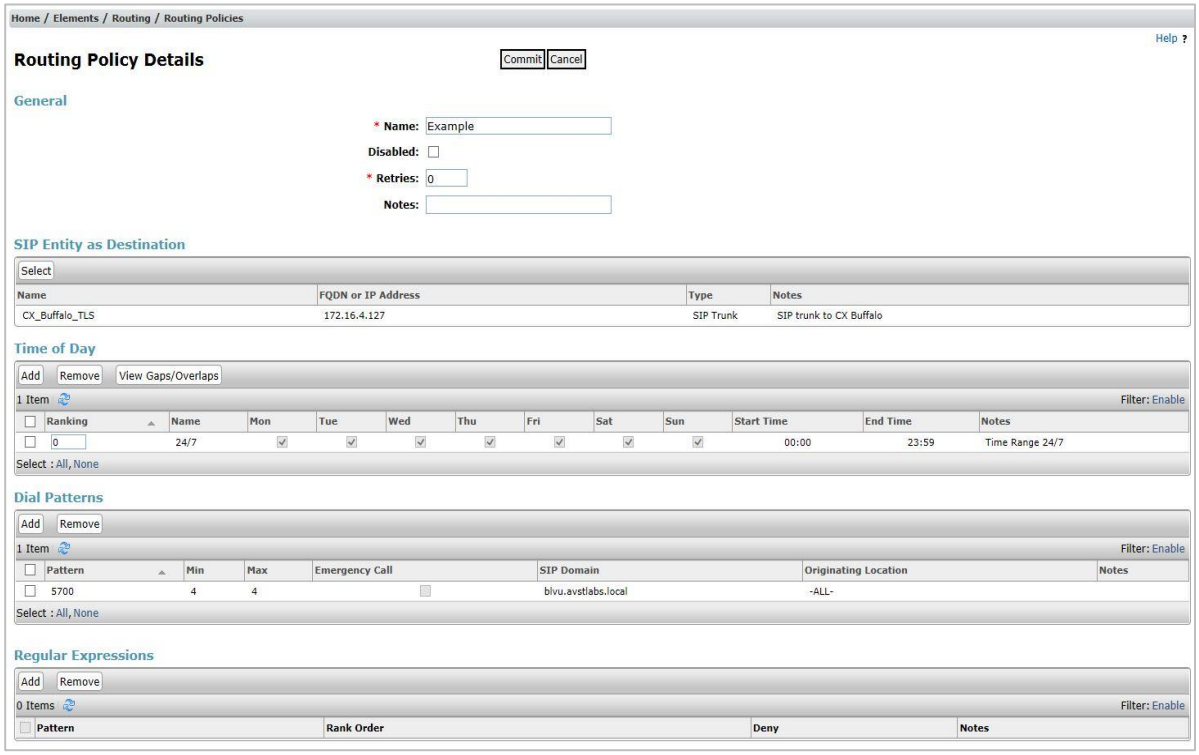


Figure 10. System Manager – Routing Policies

- To add a new Routing Policy, click **New**.
- To edit an existing Routing Policy, select the Routing Policy name, or select the Routing Policy checkbox and click **Edit**.
- On the **Routing Policy Details** page, configure the required **Name** and **Retries** fields; and the remaining fields appropriate for your organization.



Adding Avaya Trusted Certificates

Adding Trusted Certificates

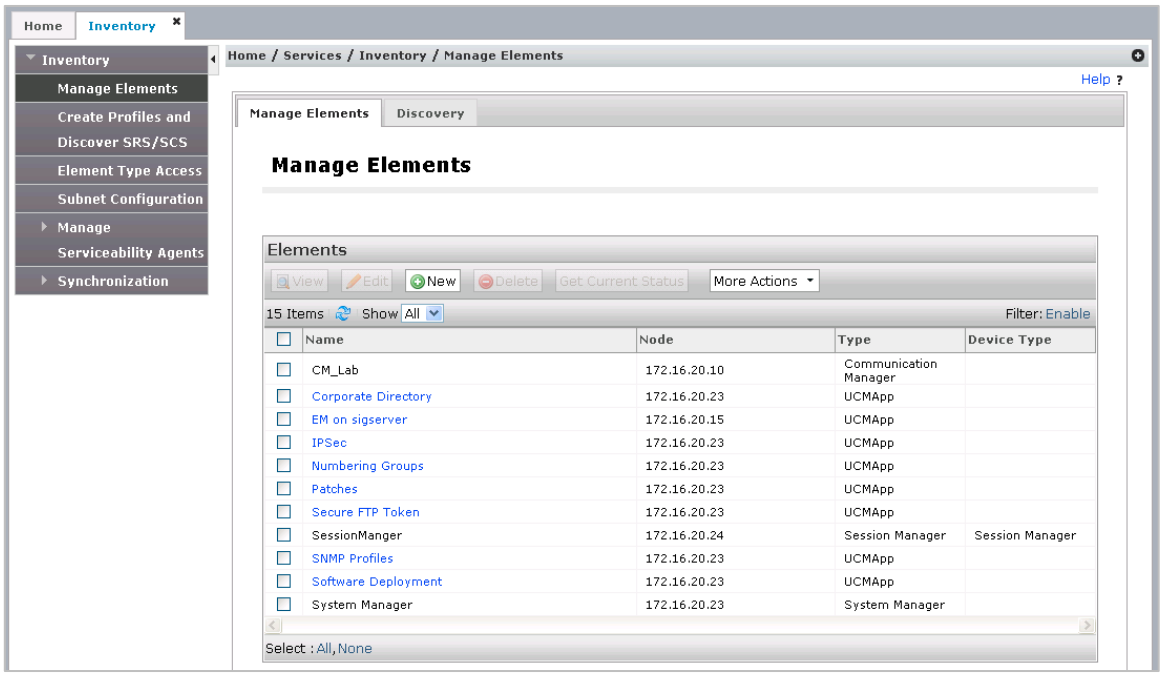
You need to import the certificates that you want to add as trusted certificate in the trust store of the application. The following are the four methods of importing a trusted certificate in the trust store for an application instance:

- Import from existing
- Import from file
- Import as PEM Certificate
- Import using TLS

You can add a trusted certificate from a list of an existing certificates, a file, a remote location using TLS connection, and by copying the content from a PEM file.

To add Trusted Certificates:

1. Log in to the System Manager, and go to **Services** > **Inventory** > **Manage Elements**. The **Manage Elements** page appears.



2. On the **Manage Elements** page, select checkbox(es) of the element(s) you want to add trusted certificates to.
3. Click the **More Actions** drop-down list, and select **Manage Trusted Certificates.**

4 On the **Manage Trusted Certificates** page, click **Add**.

5 On the **Add Trusted Certificate** page, select store type from the **Store Type** field and perform one of the following steps:

a To import certificates from existing certificates:

(1) Click **Import from existing**.

(2) Select the certificate from the **Global Trusted Certificate** section.

(3) Click **Commit**.

b To import certificates from a file:

(1) Click **Import from file**.

(2) Enter the name of the file. You can also click **Browse** to select a file.

(3) Click **Retrieve Certificate**.

(4) Click **Commit**.

c To import certificates in the PEM format:

(1) Locate the **PEM** certificate.

(2) Open the certificate in the Notepad application.

(3) Select all the contents in the file.

(4) Perform a copy operation.

(5) Click **Import as PEM** Certificate.

(6) Perform a paste operation in the box provided at the bottom of the page.

NOTE You may include the start and end tags:

" -----BEGIN CERTIFICATE-----" and" -----END CERTIFICATE----".

(7) Click **Commit**.

d To import using TLS:

(1) Click **Import using TLS**.

(2) Enter the IP address of the computer in the **IP Address** field.

(3) Enter the port of the computer in the **Port** field.

(4) Click **Retrieve Certificate**.

(5) Click **Commit**.

Setting up Avaya SRTP SIP

For a detailed example on setting up Avaya SRTP SIP, please refer to Avaya the Solution & Interoperability Test Lab Application Notes document entitled *Configuring Secure Real-Time Transport Protocol (SRTP) and G.722 Audio using Avaya 9600-Series IP Telephones running SIP and H.323 Firmware – Issue 1.0*. The document is available at: downloads.avaya.com/css/P8/documents/003954807.

Programming MiCollab AM Ports

Assign the station ports to the trunk group you have created (and have therefore included in the integration). Assign an **Extension Number** and a **Name** to each port and set the **Station Type** to **4620**.

(Page 1)

Page 1 of 5

STATION

Extension: 4002
Type: 4620
Port: S00003
Name: Test Station 4002

Lock Messages? n
Security Code:
Coverage Path 1: 57
Coverage Path 2:
Hunt-to Station:

BCC: 0
TN: 1
COR: 1
COS: 1
Tests? y

STATION OPTIONS

Loss Group: 19
Speakerphone: 2-way
Display Language: english
Survivable GK Node Name:
Survivable COR: internal
Survivable Trunk Dest? y

Time of Day Lock Table:
Personalized Ringing Pattern: 1
Message Lamp Ext: 4002
Mute Button Enabled? y
Expansion Module? n
Media Complex Ext:
IP SoftPhone? n
IP Video? n
Short/Prefixed Registration Allowed: default
Customizable Labels? y

(Page 2)

Page 2 of 5

STATION

FEATURE OPTIONS

LWC Reception: spe
LWC Activation? y
LWC Log External Calls? n
CDR Privacy? n
Redirect Notification? y
Per Button Ring Control? n
Bridged Call Alerting? n
Active Station Ringing: single

Auto Select Any Idle Appearance? n
Coverage Msg Retrieval? y
Auto Answer: none
Data Restriction? n
Idle Appearance Preference? n
Bridged Idle Line Preference? n
Restrict Last Appearance? y
EMU Login Allowed? n
Per Station CPN - Send Calling Number?
EC500 State: enabled
Audible Message Waiting? n
Display Client Redirection? n
Select Last Used Appearance? n
Coverage After Forwarding? s
Multimedia Early Answer? n
Direct IP-IP Audio Connections? y
IP Audio Hairpinning? n

H.320 Conversion? n
Service Link Mode: as-needed
Multimedia Mode: enhanced
MWI Served User Type: sip-adjunct

Emergency Location Ext: 4002 Always Use? n

(Page 3)

```
                                                          Page   3 of   5
                                  STATION

                 Conf/Trans on Primary Appearance?   n
      Bridged Appearance Origination Restriction?    n

                  Call Appearance Display Format:    disp-param-default
                                IP Phone Group ID:
Enhanced Callr-Info Display for 1-Line Phones?       n

                          ENHANCED CALL FORWARDING
                                     Forwarded Destination        Active
Unconditional For    Internal Calls To:                            n
                     External Calls To:                            n
          Busy For   Internal Calls To:                            n
                     External Calls To:                            n
      No Reply For   Internal Calls To:                            n
                     External Calls To:                            n

              SAC/CF Override:   n
```

(Page 4)

```
                                                          Page   4 of   5
                                  STATION
SITE DATA
      Room:                                        Headset?   n
      Jack:                                        Speaker?   n
     Cable:                                        Mounting:  d
     Floor:                                   Cord Length:    0
  Building:                                       Set Color:

ABBREVIATED DIALING
     List1:                 List2:                 List3:

BUTTON ASSIGNMENTS
 1:  call-appr                          5:
 2:  call-appr                          6:
 3:  call-appr                          7:
 4:                                     8:
```

Declare the ports you have defined, and any SIP-based extensions that MiCollab AM subscribers use, as parts of an external integration.

To do this, enter the command ***change off-pbx-telephone station-mapping <number>***, where ***<number>*** is the station number for any port involved in the integration.

The command displays a table that you can use to configure all of the station ports you need to change. Associate all of these ports with the trunk group you defined earlier, as the following example demonstrates.

(Page 1)

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	

Configuring the SIP Entities on Avaya Servers

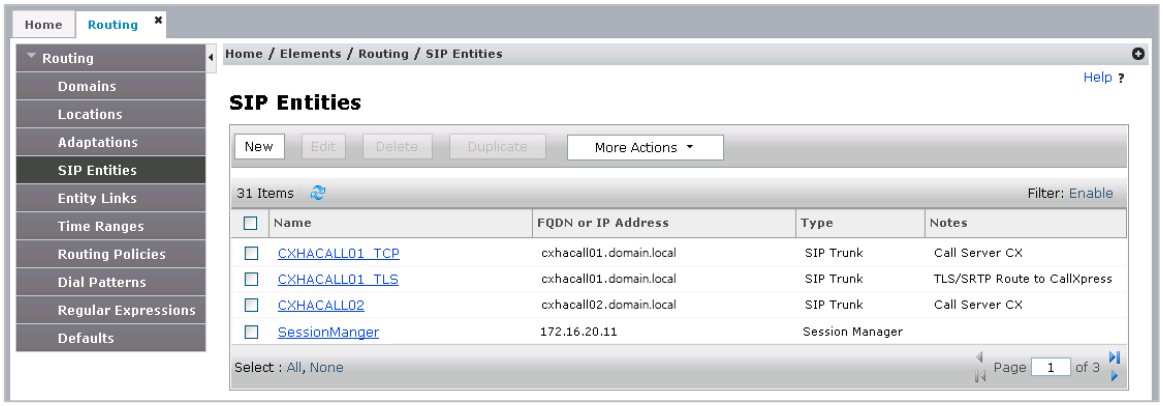
Verify the connection between the Communications Manager and Session Manager servers on the Session Manager server. Make sure the Communication Manager server Interface reflects the same IP addresses as the Media Server Interface.

Configure a SIP Entity for the Communication Manager server and a SIP Entity for the Session Manager server.

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

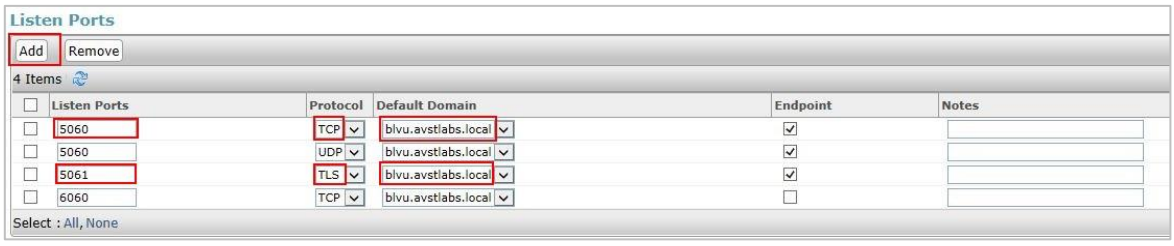
To configure the SIP Entities:

1. Log in to the System Manager, and go to **Elements** > **Routing** > **SIP Entities**. The **SIP Entities** page appears.



2 From the SIP Entities table, select **Session Manager**, or select the **Session Manager** checkbox and then click **Edit**. The **SIP Entity Details** page appears.

3 On the **SIP Entity Details** page, go to the **Port** section, and then assign the **Listen Port** number, select **TCP**, **TLS**, or **UDP** as the **Protocol**, and select the **Default Domain**.

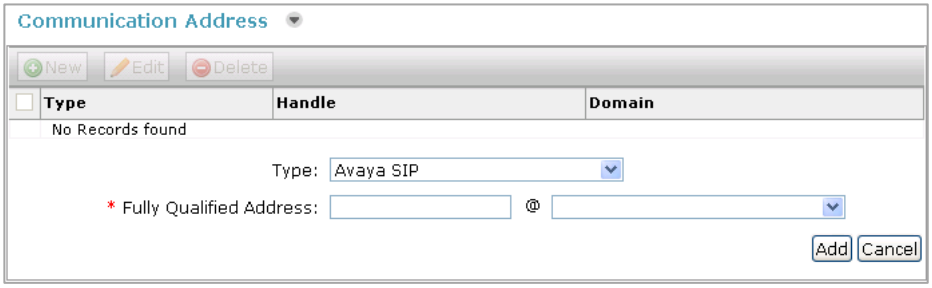


IMPORTANT The port number and the protocol you enter here must match the SIP Server Port and the Transport for Outgoing SIP Message of the Required Parameters fields on the MiCollab AM **Integration Options** dialog box.

The default protocol is **TCP** and the default port number is **5060**. For more information, refer to the Configuring MiCollab AM section.

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

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

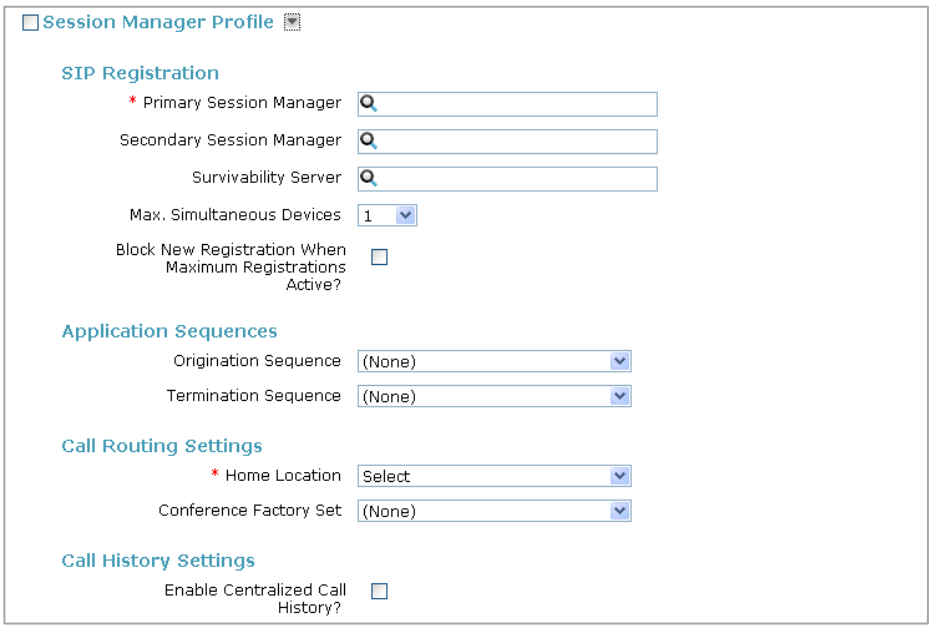


6 From the **Type** drop-down menu, select **Avaya SIP.**

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

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

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



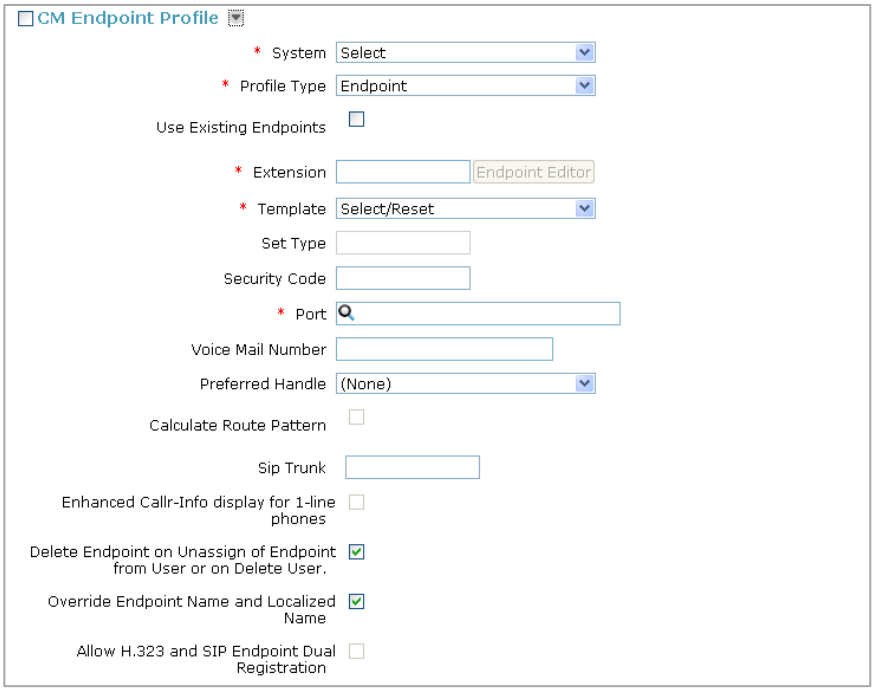
10 In the **Session Manager Profile** section, fill in the following options:

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.

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



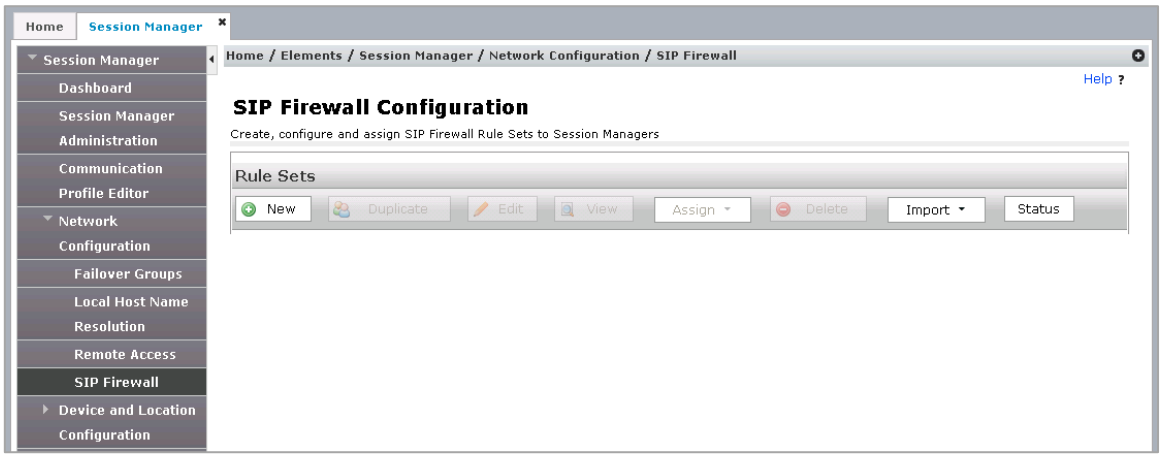
12 In the **CM Endpoint Profile** section, fill in the appropriate options for **System**, **Profile Type**, **Extension**, **Template**, **Security Code**, **Port**, and **Voice Mail Number**.

Configuring the Session Manager Firewall

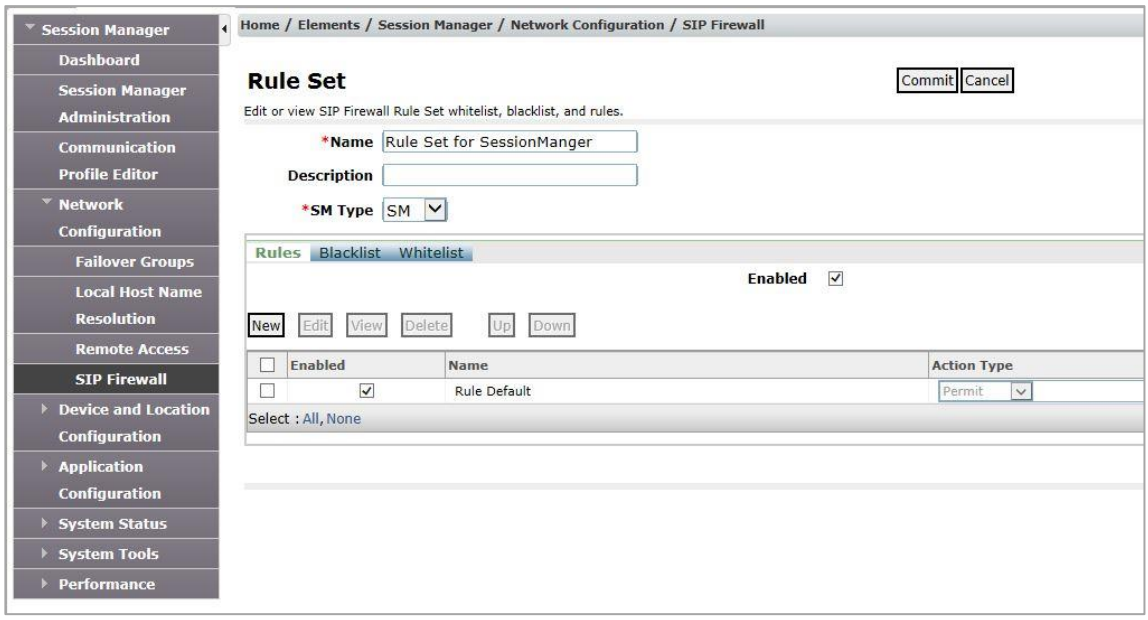
Verify that the MiCollab AM server's IP address is not blocked by the Session Manager firewall. If there is more than one Call Server participating in the integration, ensure that the Session Manager server does not block the IP Address of any Call Server.

To configure the Firewall:

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

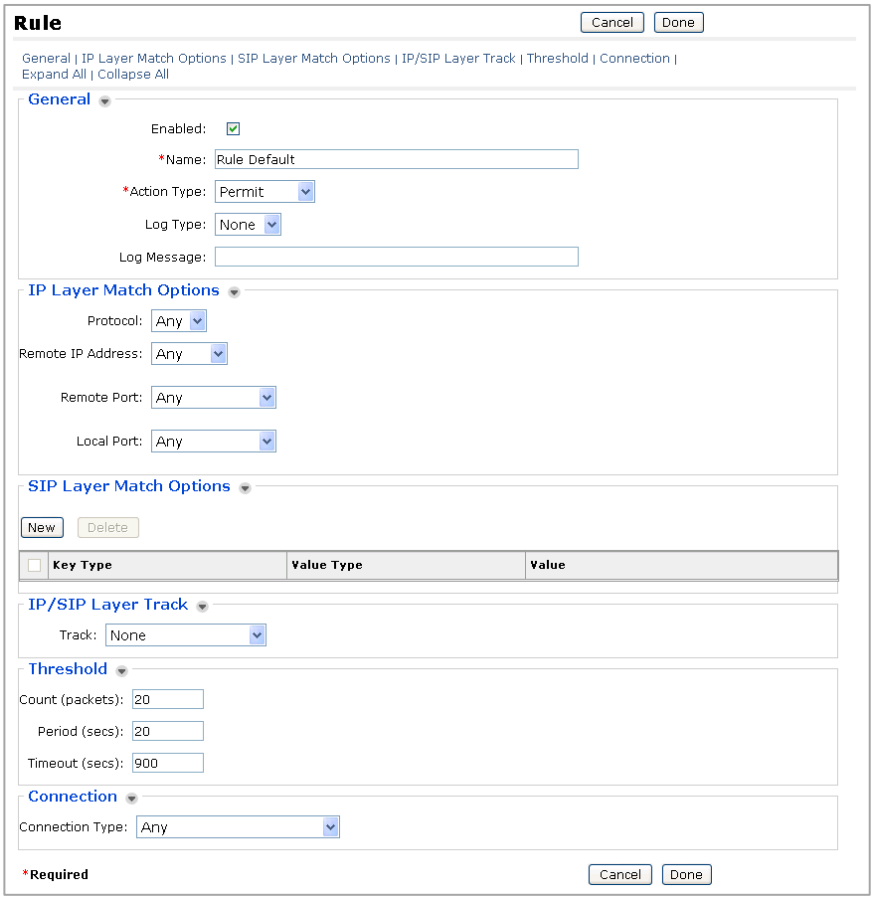


14 On the **SIP Firewall Configuration** page, in the **Rule Sets** section, click **New**. The **Rule Set** page appears.



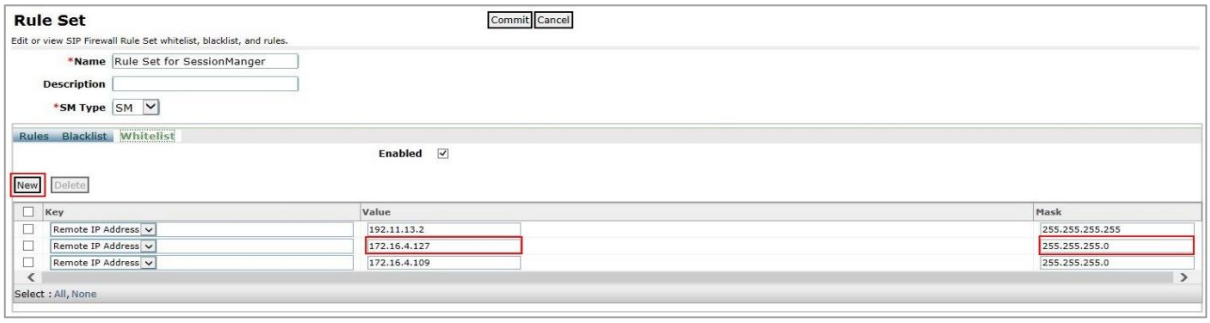
15 In the **Name** field, select or type *Rule Set for SessionManager*.

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



17 On the **Rule** page, configure the firewall appropriately to allow access to each Call Server in the integration. When finished, click **Done**.

18 Click the **Whitelist** tab and click **New**.



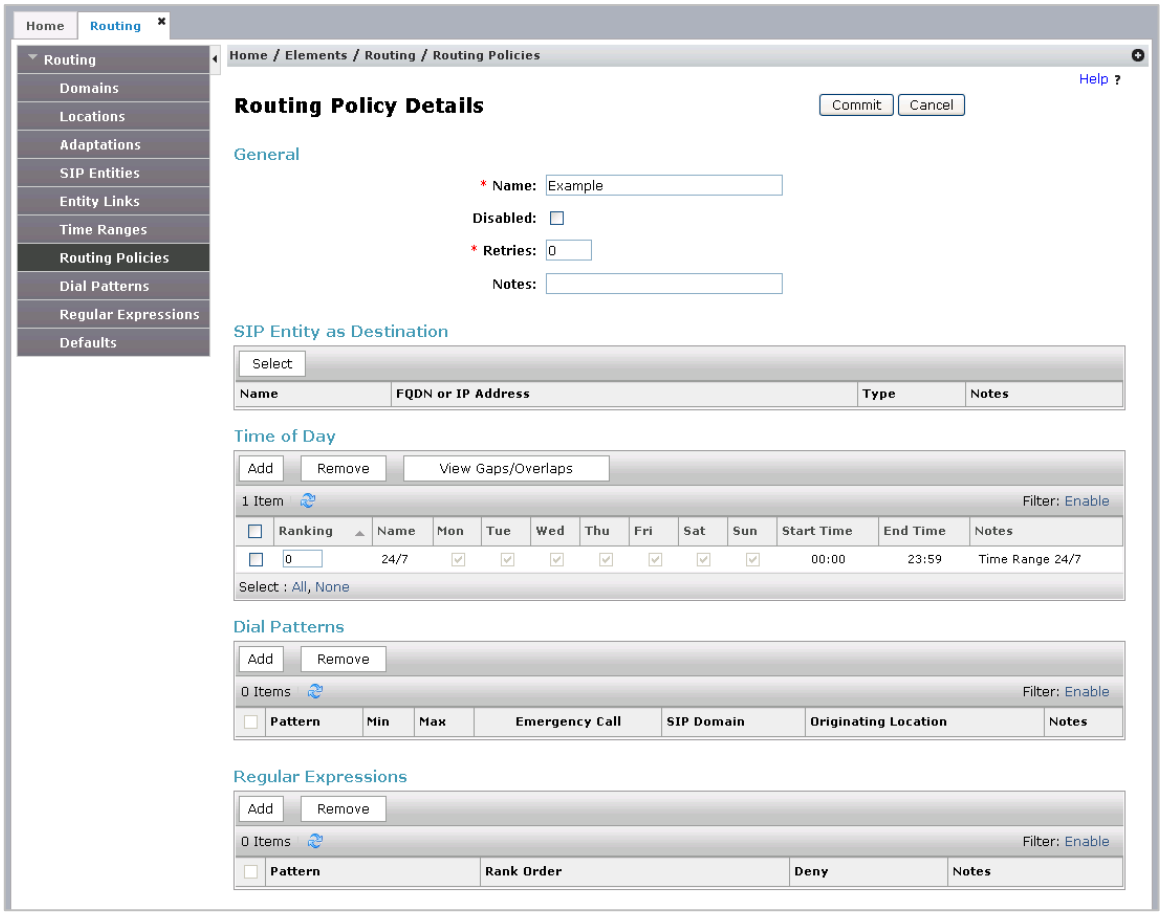
19 Define an IP address to ensure that an IP address is not being blocked by a firewall. Click **Commit**.

Configuring the Routing Policies

Configure the routing policies and the dialing pattern for the MiCollab AM hunt group and the non-SIP subscriber directory number range.

To configure the routing policies:

1. Log in to the System Manager, and go to **Elements** > **Routing** > **Routing Policies**. The **Routing Policies** page appears.
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, enter the name for the policy and number of retries.
4. In the **SIP Entity as Destination** and **Dial Pattern** sections, configure the options for the MiCollab AM hunt group number and the non-SIP subscriber directory number range according to the requirements of the site. This enables the non-SIP calls to route to the Communication Manager.

> **IMPORTANT** When you add user definitions for the MiCollab AM ports, you must assign the same password to all users and all ports. If you do not, the integration cannot function correctly.

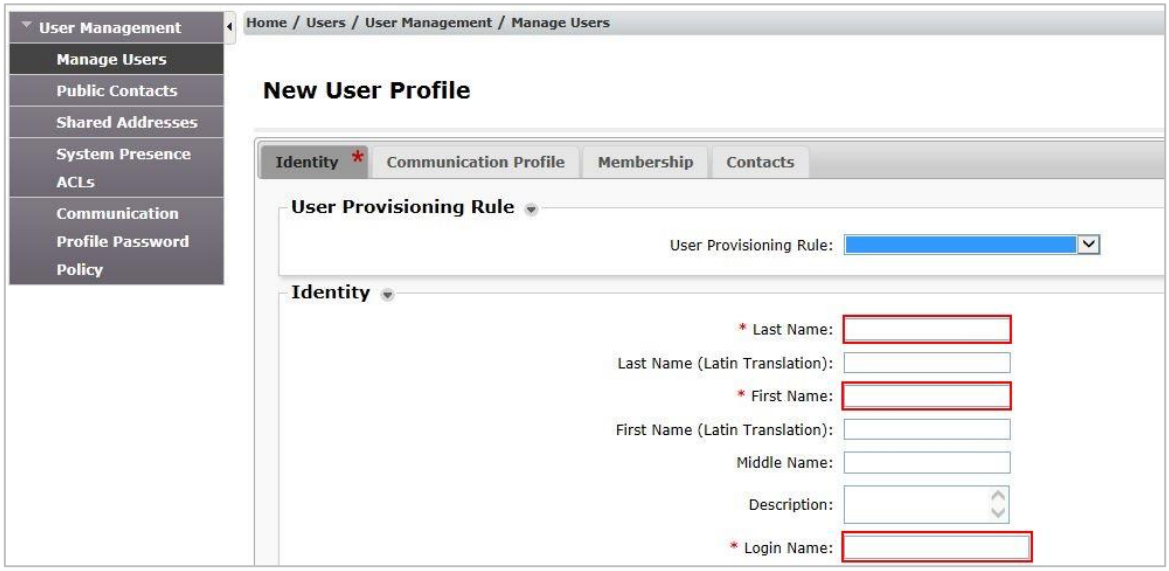
5. Click **Commit** to save the changes.

Adding the MiCollab AM Port User Definitions

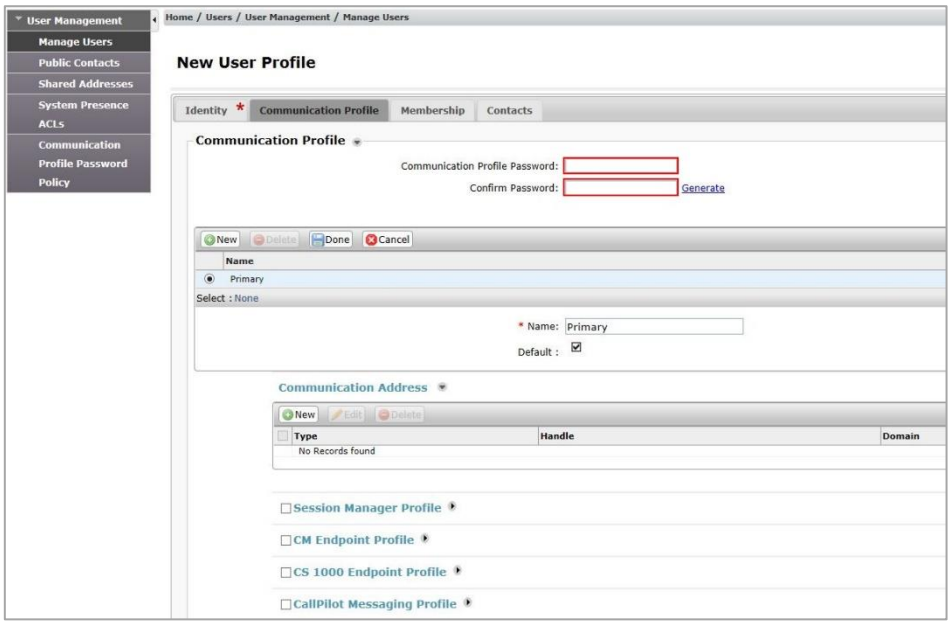
Add a user definition for each MiCollab AM port in the integration.

To add a user definition:

1. Log in to the System Manager, and go to **Users** > **User Management** > **Manage Users**. The **User Management** page appears.
2. On the **User Management** page, click **New**. The **New User Profile** page displays in the **Identity** tab.



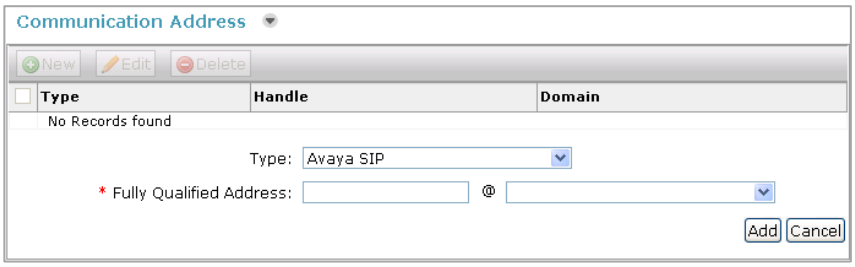
3. In the **Identity** tab, fill in the appropriate fields.
4. Click the **Communication Profile** tab.



5 In the **Communication Profile** section, enter the same numeric password for MiCollab AM.

> **NOTE** The password is required later to configure the MiCollab AM integration.

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

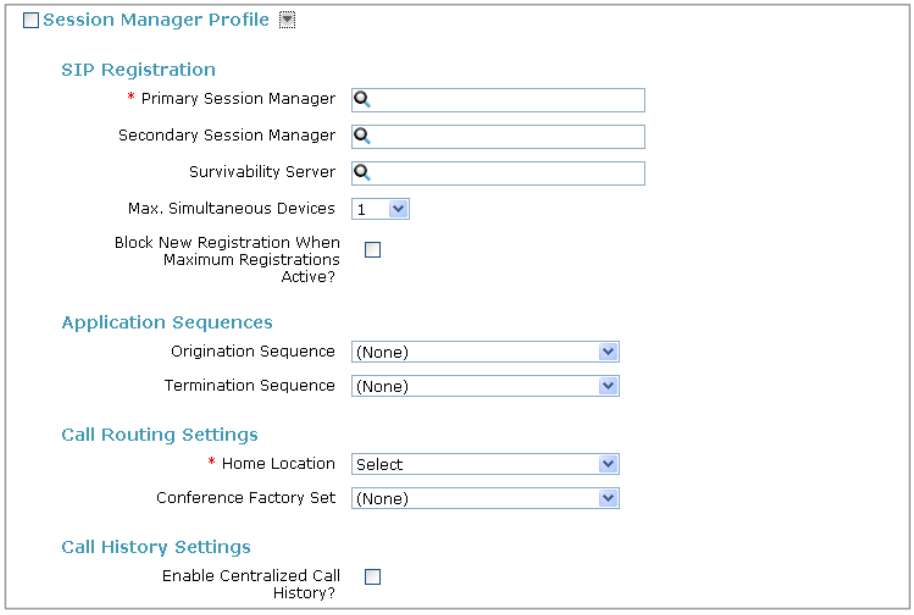


7 From the **Type** drop-down menu, select **Avaya SIP.**

8 In the **Fully Qualified Address** fields, enter the extension number assigned to the port and the domain. And then click **Add**.

> **NOTE** Assign each port the same extension number as you assigned it in the ASA configuration screens.

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



10 In the **Session Manager Profile** section:

- **a** In the **SIP Registration** section, select the **Primary Session Manager**.
- **b** In the **Call Routing Settings** section, select the **Home Location**.

11 No administration is required for the **CM Endpoint Profile** section.

12 Click **Commit**.

Creating a Hunt Group and Pilot Number

In order to create a hunt group and pilot number:

- Define a Hunt Group for MiCollab AM and assign a Pilot Number to it that is not associated with any port or extension.
- Set the ISDN/SIP Caller Display to mbr-name to allow the stations in the group to display the name of the group member receiving the call.
- Add all MiCollab AM port extensions to the new hunt group.

The following examples show a typical hunt group configuration for this integration.

(Page 1)

```
                                                              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)

```
                                                              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)

```
                                                                    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 under Creating a SIP Trunk Group.

IMPORTANT You must deactivate Secure SIP in this route pattern.

```
                                                                    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 hunt pilot number is a valid dialed string that maps to the route pattern you have defined for the MiCollab AM hunt group, as shown in the following example:

12 Items

	Dialed String	Total Min	Total max	Route Pattern	Call Type	Node Number
○	5300	4	4	53	aar	
○	5400	4	4	54	aar	
○	5500	4	4	27	aar	
○	5600	4	4	1	aar	
○	5700	4	4	57	aar	
○	5800	4	4	58	aar	
○	5900	4	4	59	aar	
○	6	7	7	999	aar	
○	6000	4	4	99	unku	
○	7	7	7	999	aar	
○	7000	4	4	99	aar	
○	8	7	7	999	aar	

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:

change aar digit-conversion 0 Page 1 of 2

AAR DIGIT CONVERSION TABLE

Location: all Percent Full: 0

Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	ANI Req
0	1	28	0		ars	y	n
1	4	28	0		ars	y	n
4	4	4	0		ext	y	n
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
							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 under the Creating a Route Pattern section.

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 SIP phones.

For more information, refer to *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* available at: downloads.avaya.com/css/P8/documents/100169223.

The document 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 examples in Step 2.
2. Make the **MWI LAMP Ext** number the same as the station's extension number, and set the **Coverage Path 1** to the one you created earlier.
3. Set the **MWI Served User Type** as, **sip-adjunct**, and then associate the station with the Trunk Group you defined previously.

   (Page 1)

```
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
```

(Page 2)

```
display station 4021                                          Page   2 of   6
                                    STATION
FEATURE OPTIONS
            LWC Reception:   spe
           LWC Activation?   y                    Coverage Msg Retrieval?   y
                                                              Auto Answer:   none
              CDR Privacy?   n                          Data Restriction?   n
                                              Idle Appearance Preference?   n
 Per Button Ring Control?    n               Bridged Idle Line Preference?   n
   Bridged Call Alerting?    n                  Restrict Last Appearance?   n
  Active Station Ringing:    single

        H.320 Conversion?   n          Per Station CPN - Send Calling Number?
                                                     EC500 State:   enabled

    MWI Served User Type:   sip-adjunct

                                                Coverage After Forwarding?   s

                                              Direct IP-IP Audio Connections?   y
  Emergency Location Ext:   4021        Always Use?   n IP Audio Hairpinning?   n
```

4 Associate the station with the SIP trunk. This is required for MWI purposes.

(Page 6)

```
                                                              Page   6 of   6
                                    STATION
SIP FEATURE OPTIONS

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

5 Add the station to the *off-pbx-telephone station-mapping*. **AAR** is used for routing of 4011 and 4012. In the **AAR** form:

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	

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

Page 1 of 2

NUMBERING - PUBLIC/UNKNOWN FORMAT

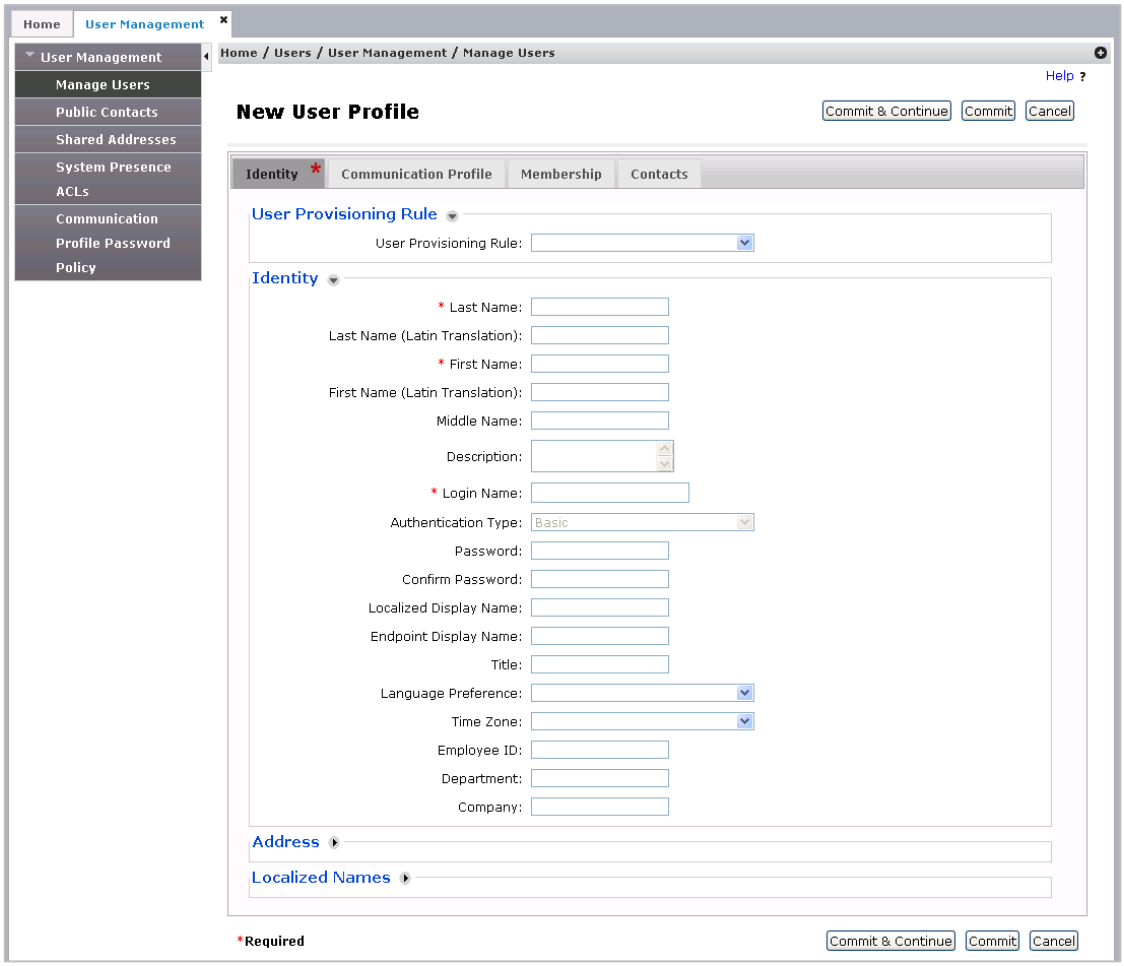
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len
4	4			4
5	4	27		4
4	5	1		4
6	8		88	8
7	8	11	555	10
4	4400	11	425111	10
4	5700	57		4
4	5800	58		4

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.

7 To add new users, log in to the System Manager, and go to **Users** > **User Management** > **Manage Users**. And the click **New**. The **New User Profile** page displays in the **Identity** tab.



8 In the **Identity** tab, add in the name and password as required.

9 Click the **Communication Profile** tab.

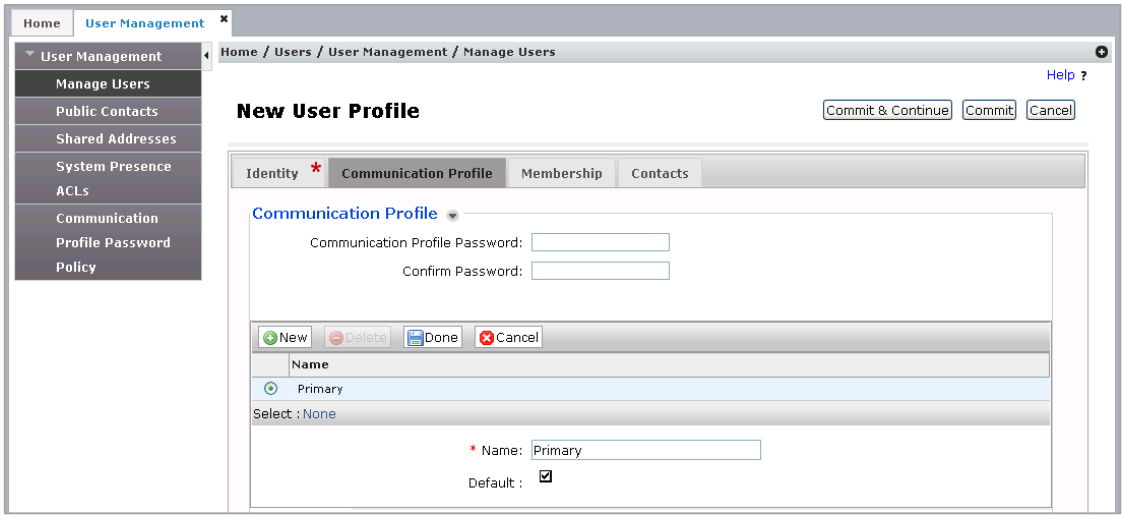
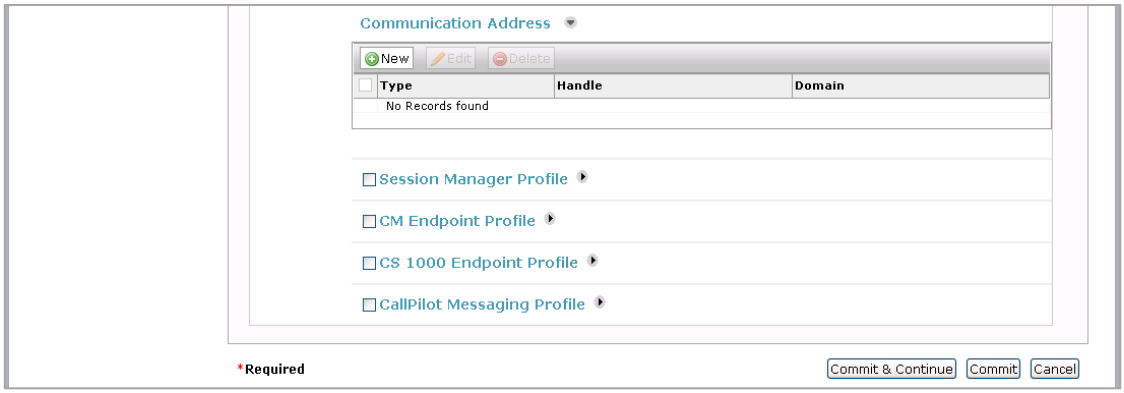


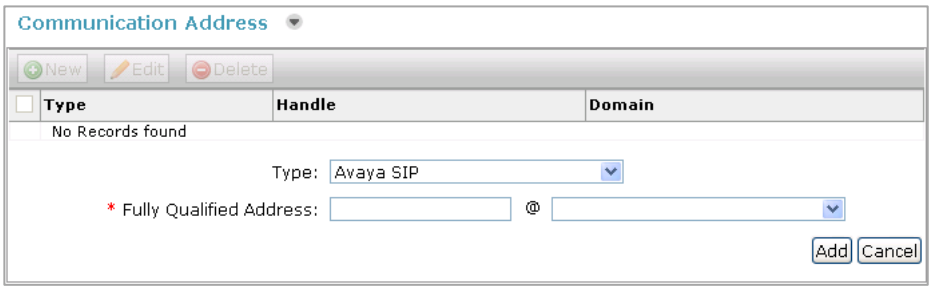
Image continues on next page

Image continued from previous page



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

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

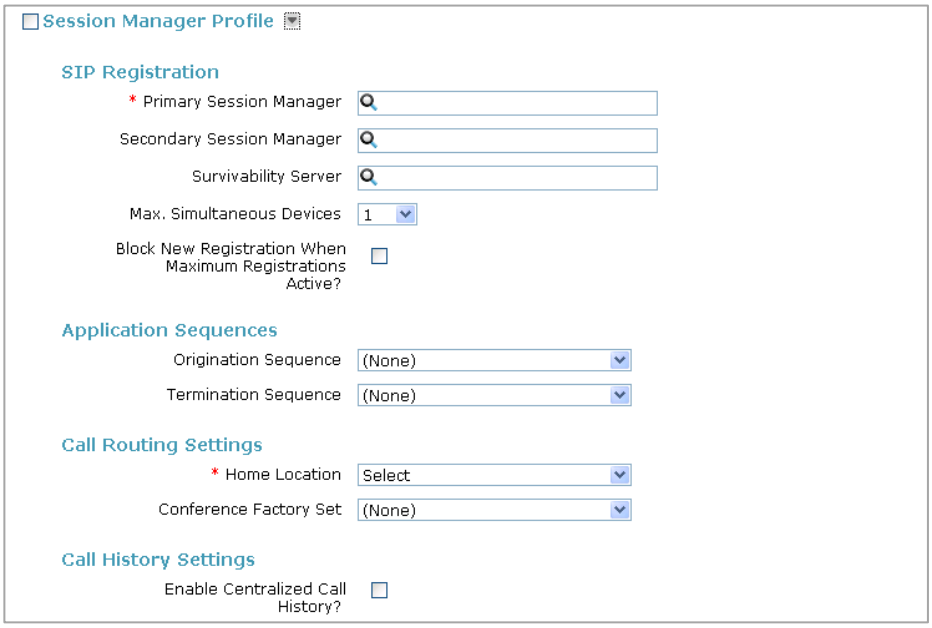


12 From the **Type** drop-down menu, select **Avaya SIP.**

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

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

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



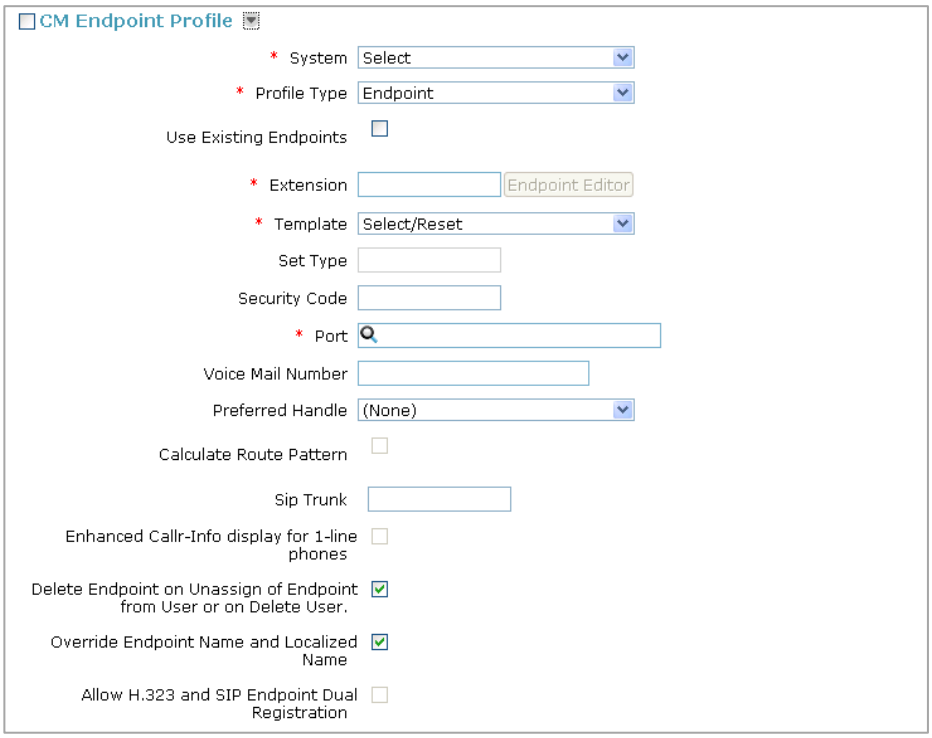
16 In the **Session Manager Profile** section, fill in the following options:

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.

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



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

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.

IMPORTANT During the integration process, you would be required to import certificate files to the MiCollab AM system. Prior to configuring MiCollab AM, copy the certificate files (**Telephonyserversipcert.pem** and **Telephonyserversipkey.pem**) to local MiCollab AM server of designated certificate repository.

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 with the integration for the first time:

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 displays for the virtual board configuration.
3. In the **Board Options** dialog box, configure the following options:
   - **a** From the **Manufacturer** drop-down list, select **Virtual**.

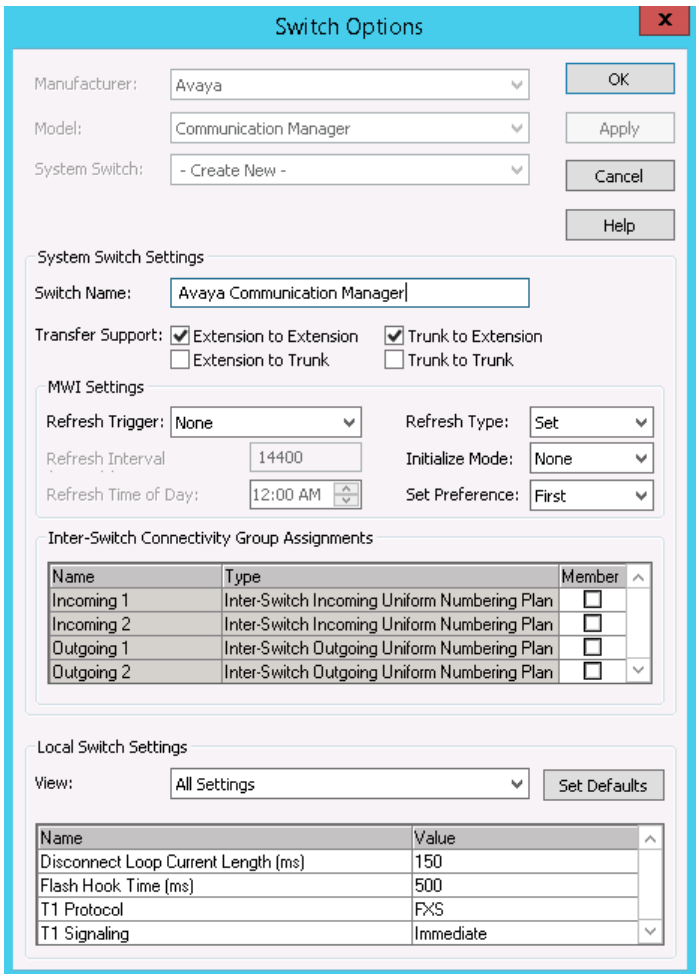
b From the **Model** drop-down list, select **SIP STACK**.

c In the **Name** field, the name for this board is automatically generated. Enter a new name if necessary.

d From the **Protocol** drop-down list, select **SIP IP RTP**.

e In the **Number of Lines** field, enter the number of lines this board uses. The total number of lines is limited by the capacity of the board and the number of **Available Line Licenses**.

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

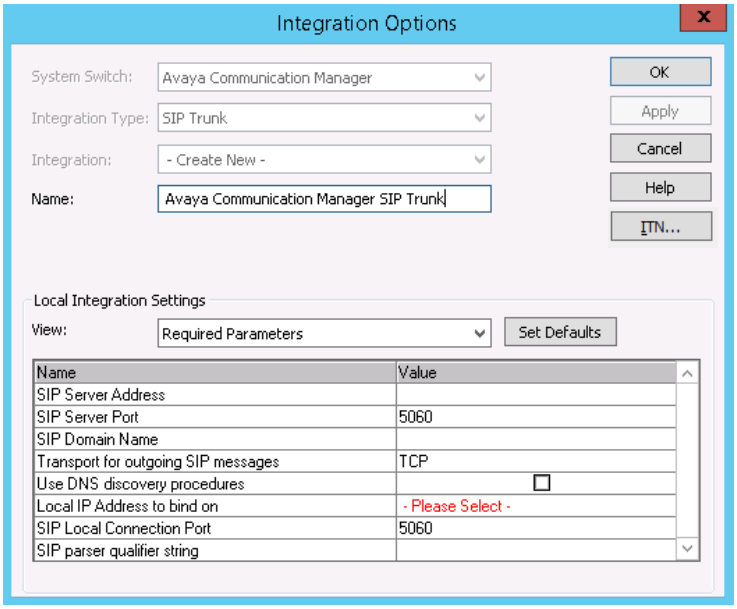


5 If necessary, make any changes to the default settings your site requires in the **Switch Options** dialog box.

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

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

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



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

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

Table 4. Required Parameters View – Integration Options

Field	Required Value
SIP Server Address	Enter the IP address of the Session Manager server.
SIP Server Port	Enter the port number on which the Session Manager listens for SIP messages. This port must match the Session Manager port. The default port number is 5060.
SIP Domain Name	Enter the SIP domain name. This case-sensitive value must be the same as the Far-End Domain Name in the signaling group. **NOTE** This value is case-sensitive.
Transport for outgoing SIP messages	Enter TCP or UDP (TCP is the default value.)
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 TCP port 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 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.
PBX Password	Enter the password that you assigned to the user definitions for the integrated ports earlier in this document.
Media packet size (milliseconds)	MiCollab AM sends/receives packets containing the number of milliseconds worth of audio data set here. The default value is 20.

b In the **Local Integration Settings** section, select the **Media Settings** view, and configure the following options:

- 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 Critical Application Considerations section.

c In the **Local Integration Settings** section, select the **Connection Security Settings** view, and configure the following options:

IMPORTANT Make sure that you have copied the certificate files to local MiCollab AM server of designated certificate repository.

(1) Copy certificate files (**Telephonyserversipcert.pem** and **Telephonyserversipkey.pem**) to local MiCollab AM server of designated certificate repository.

(2) In the settings table, select the **Enable TLS** checkbox.

(3) Below the settings table, click **Add Trusted SIP Server Address**. This will add a line **SIP Server Address** to the settings table.

(4) In the **SIP Server Address** field, enter the address of the server.

(5) If the **Show thumbprint properties** checkbox is selected, deselect the checkbox. This will show the **Local Certificate FileName** and **Local Private Key FileName** fields in the settings table.

NOTE If you want retain the **Show thumbprint properties** checkbox as selected, you must have your ***cert.pem** and ***key.pem** files in the store.

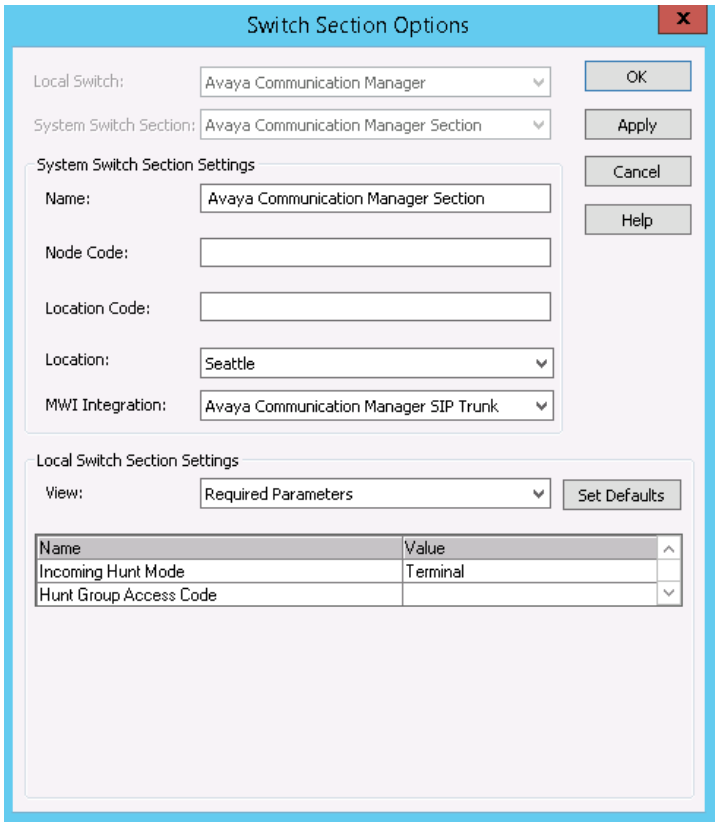
(6) In the **Local Certificate FileName** field, click the ... (browse) icon to import the ***cert.pem** connection security settings file.

(7) In the **Local Private Key FileName** field, click the ... (browse) icon to import the ***.key.pem** connection security settings file.

(8) Click **Apply** to save your changes.

d In the **Local Integration Settings** section, select the **Software DTMF Detection Settings** view, and confirm the **DTMF Detection Type** parameter is set to **Hardware**, the default value.

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



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

a In the **Local Switch Section Settings** section, select the **Required Parameters** View.

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

> **NOTE** Select the hunt mode that matches the hunt mode type you created in IP PBX programming.

c In **Hunt Group Access Code** box, type the hunt pilot number you defined earlier in the Creating a Hunt Group and Pilot Number section.

d Click **OK**.

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

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

12 In the table from the **Lines** tab, enter the extension number of each integrated line on the Call Server.

> **IMPORTANT** You must enter the PBX extension numbers that the Call Server is configured to answer or the integration will fail. The extension numbers are registered as SIP stations with the IP PBX during system startup.

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

Configuring Existing MiCollab AM for the Integration

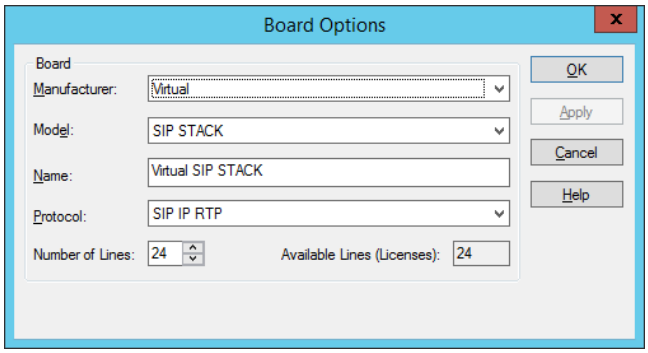
To configure exiting MiCollab AM for the telephone integration:

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

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

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

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



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

b From the **Model** drop-down list, select **SIP STACK**.

c In the **Name** field, the name for this board is automatically generated. Enter a new name if necessary.

d From the **Protocol** drop-down list, select **SIP IP RTP**.

e In the **Number of Lines** field, enter the number of lines this board uses. The total number of lines is limited by the capacity of the board and the number of **Available Line Licenses**.

f Click **OK**.

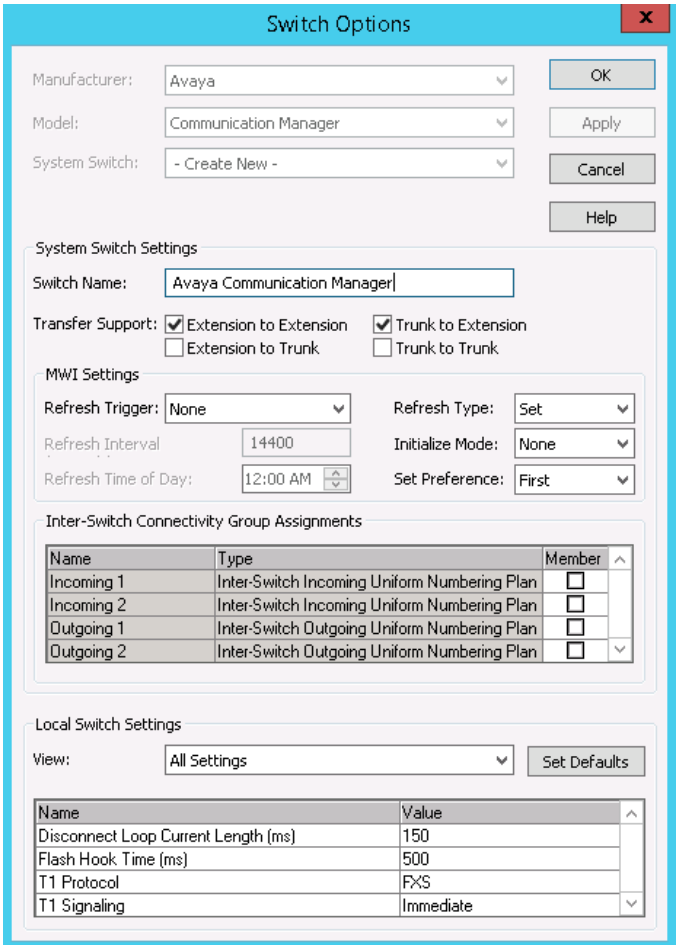
4 Select the **Switches** tab, and click the **Add** button. The **Switch Integration Data Setup** dialog box appears.

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**.

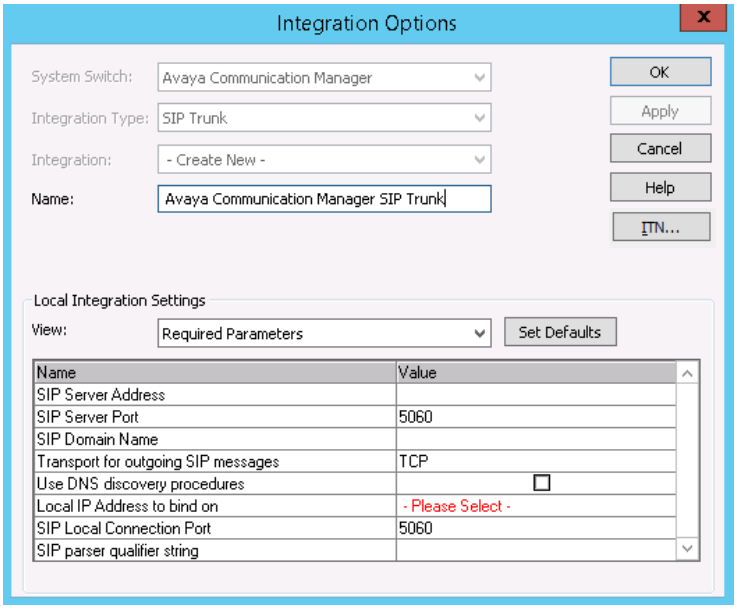
5 Click **OK**. The **Switch Options** dialog box appears.



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 Settings** section, select the **Required Parameters** view, and configure the following options:

Table 5. Required Parameters View – Integration Options

Field	Required Value
SIP Server Address	Enter the IP address of the Session Manager server.
SIP Server Port	Enter the port number on which the Session Manager listens for SIP messages. This port must match the Session Manager port. The default port number is 5060.
SIP Domain Name	Enter the SIP domain name. This case-sensitive value must be the same as the Far-End Domain Name in the signaling group. **NOTE** This value is case-sensitive.
Transport for outgoing SIP messages	Enter TCP or UDP (TCP is the default value.)
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 TCP port 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 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.
PBX Password	Enter the password that you assigned to the user definitions for the integrated ports earlier in this document.
Media packet size (milliseconds)	MiCollab AM sends/receives packets containing the number of milliseconds worth of audio data set here. The default value is 20.

b In the **Local Integration Settings** section, select the **Media Settings** view, and configure the following options:

- 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 Critical Application Considerations section.

c In the **Local Integration Settings** section, select the **Connection Security Settings** view, and configure the following options:

IMPORTANT Make sure that you have copied the certificate files to local MiCollab AM server of designated certificate repository.

(1) Copy certificate files (**Telephonyserversipcert.pem** and **Telephonyserversipkey.pem**) to local MiCollab AM server of designated certificate repository.

(2) In the settings table, select the **Enable TLS** checkbox.

(3) Below the settings table, click **Add Trusted SIP Server Address**. This will add a line **SIP Server Address** to the settings table.

(4) In the **SIP Server Address** field, enter the address of the server.

(5) If the **Show thumbprint properties** checkbox is selected, deselect the checkbox. This will show the **Local Certificate FileName** and **Local Private Key FileName** fields in the settings table.

NOTE If you want retain the **Show thumbprint properties** checkbox as selected, you must have your ***cert.pem** and ***key.pem** files in the store.

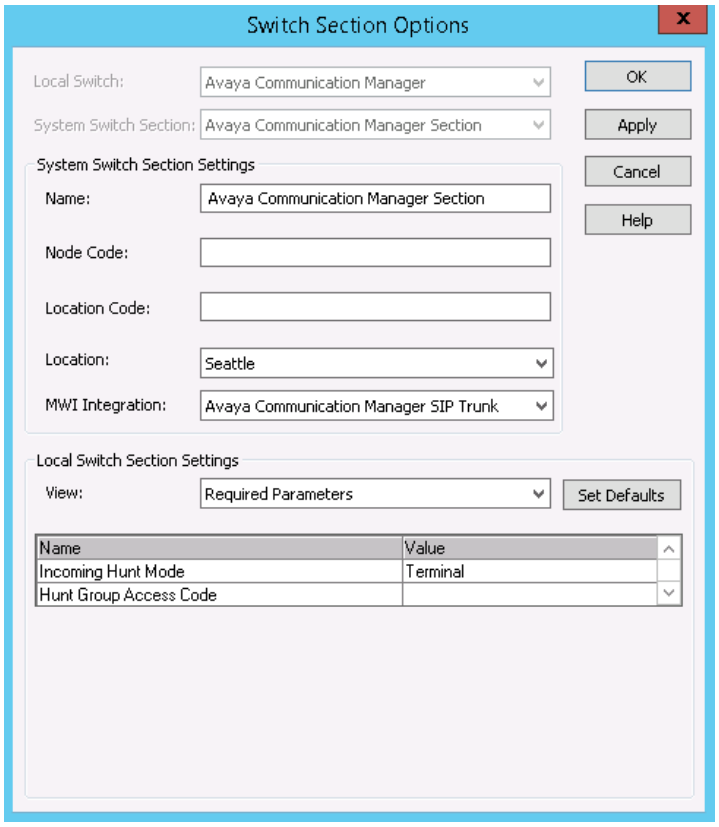
(6) In the **Local Certificate FileName** field, click the ... (browse) icon to import the ***cert.pem** connection security settings file.

(7) In the **Local Private Key FileName** field, click the ... (browse) icon to import the ***.key.pem** connection security settings file.

(8) Click **Apply** to save your changes.

d In the **Local Integration Settings** section, select the **Software DTMF Detection Settings** view, and confirm the **DTMF Detection Type** parameter is set to **Hardware**, the default value.

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



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

a In the **Local Switch Section Settings** section, select the **Required Parameters** view.

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

> **NOTE** Select the hunt mode that matches the hunt mode type you created in IP PBX programming.

c In **Hunt Group Access Code** box, type the hunt pilot number you defined earlier in the Creating a Hunt Group and Pilot Number section.

d Click **OK**.

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

12 Select the **Lines** tab.

13 In the table from the **Lines** tab, configure callouts for the application. For information on configuring callout settings, see the topic *Configuring Callout Settings*, in the online help system.

IMPORTANT You must enter the PBX extension numbers that the Call Server is configured to answer or the integration will fail. The extension numbers are registered as SIP stations with the IP PBX during system startup.

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

Configuring MiCollab AM for SIP Failover

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

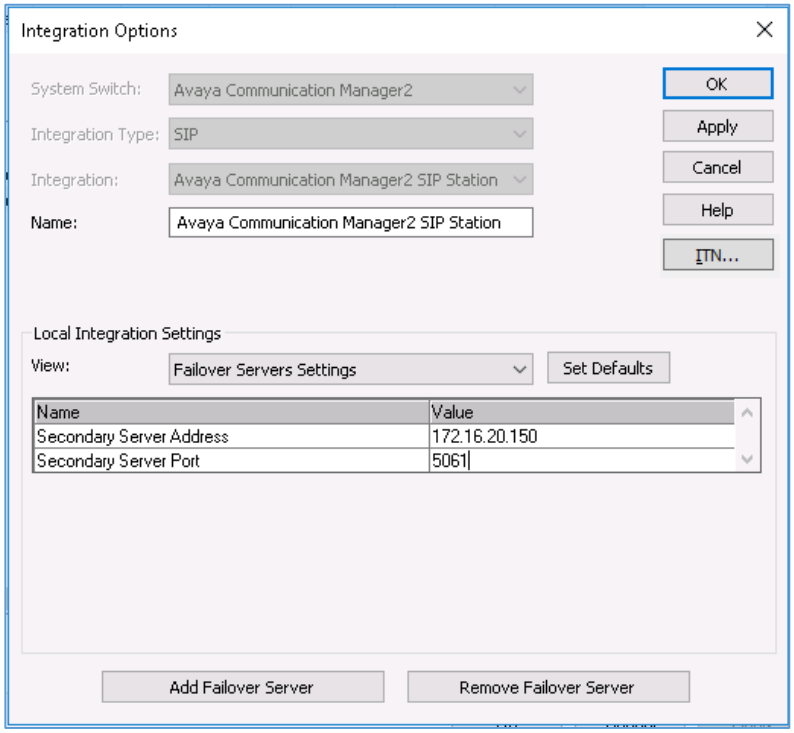
To add a SIP failover server:

1. From **MiCollab AM Configuration**, click the **Integrations** tab.
2. From the **Integrations** list, select your integration, and then click **Edit**.
3. In the **Integration Options** dialog box, go to the **Local Integration Settings** section.
4. From the **View** 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** for LSS and **5061** for a Survivable Core Server (formerly ESS).



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

Windows Server 2016 / 2019

To change the binding order of multiple NICs:

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

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

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

Configuring Quality of Service (QoS)

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

Table 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