Crestron Mercury® Tabletop Conference System (CCS-UC-1 & CCS-UC-1-X)

TLS Secure SIP Endpoint with Avaya Aura® 8.0 Communication Manager

Configuration Guide

Prepared by tekVizion for Crestron Electronics, Inc.

Original Instructions

The U.S. English version of this document is the original instructions.
All other languages are a translation of the original instructions.

Crestron Electronics, Inc.

15 Volvo Drive, Rockleigh, NJ 07647

Tel: 888.CRESTRON

www.crestron.com

tekVizion

3701 W. Plano Parkway

Suite 300, Plano, TX 75075

Tel: + 1 214-242-5900

Contents

Revision History

Revision	Date	Author	Description
1.0	January 5, 2021	tekVizion	Initial Release

Introduction

This configuration guide describes the necessary procedure to configure a Crestron Mercury® device to register to the Avaya Aura® Communication Manager as a Secure SIP Endpoint.

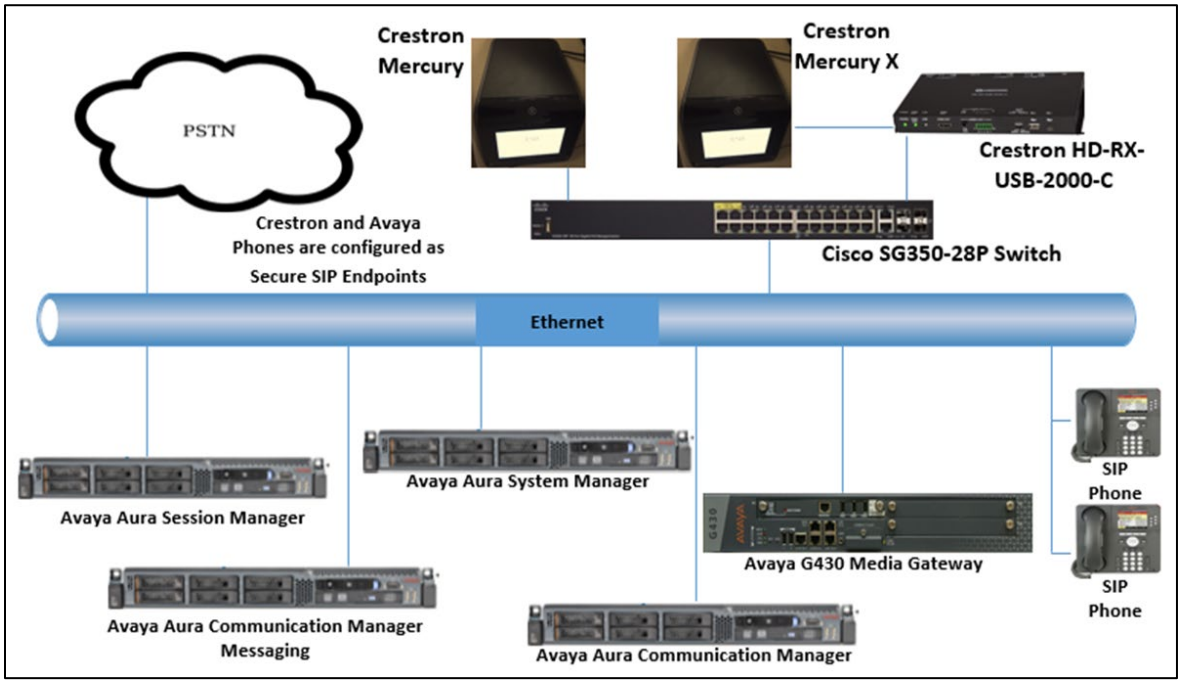
Audience

This document is intended for users attempting to configure and use Crestron Mercury as Secure SIP Endpoints registering to Avaya Aura Communication Manager 8.0.1.1.

Topology

The network topology for the Crestron Mercury Endpoint to operate with Avaya Aura is shown below.

Crestron Mercury: SIP Endpoint Integration with Avaya: Reference Network



The lab network consists of the following components:

- Avaya Aura Communication Manager
- Avaya Aura Session Manager
- Avaya Aura System Manager
- Avaya G430 Media Gateway
- Avaya Aura Communication Manager Messaging
- Avaya® SIP phones
- Crestron Mercury CCS-UC-1
- Crestron Mercury CCS-UC-1-X
- Cisco® SG350-28P Switch (VLAN Tagging)

Software Requirements

- Avaya Aura Communication manager v 8.0.1.1
- Avaya Aura Communication Manager Messaging v 7.0.0.1.441.1
- Avaya Aura System Manager v 8.0.1.1
- Avaya Aura Session Manager v 8.0.1.1
- Avaya g430 Media Gateway v 40.25.0
- Crestron Mercury devices v1.4647.00005 & 1.4647.00006
- Cisco SG350-28P Switch v 2.4.5.71

Hardware Requirements

- Cisco UCS-C240-M3S and VMware® Host software running ESXi 5.5
- Avaya components either in a virtual environment or via separate hardware servers
  - Avaya Aura Communication Manager
  - Avaya Aura System Manager
  - Avaya Aura Session Manager
  - Avaya G430 Media Gateway
  - Avaya Aura Communication Manager Messaging
- PSTN Gateway for PSTN Calling (Cisco 3845)
- Avaya phones (2) in SIP mode
- Crestron Mercury (CCS-UC-1)
- Crestron Mercury X (CCS-UC-1-X)
- Cisco SG350-28P Switch –Provides VLAN Tagging Configuration to Mercury

Product Description

The Crestron Mercury device is a complete solution for conference rooms. It acts as an all-in-one touch screen, speakerphone and AirMedia® wireless presentation product for conference rooms.

Call dialing options on this device include Bluetooth® connectivity, USB and regular audio using a dial pad, though each dialing option is exclusive.

This device can be discovered via Crestron Toolbox™ software, though most of the configuration is performed via a local web interface. An Ethernet port on the device is used to provide power and network connectivity to make audio calls via SIP.

Summary

The Crestron Mercury CCS-UC-1 & CCS-UC-1-X phones in TLS Secure mode are configured on the Avaya Aura as SIP endpoints. The phones successfully register to the Avaya Aura SM with digest authentication after establishing a TLS Secure connection with the Avaya Aura PBX.

The sections below describe the features that are supported/not supported and known issues/limitations on the Crestron Mercury phone.

Features Supported

- VLAN Tagging
- Registration with Digest Authentication
- Basic Calls with G711u, G711a and G729 codecs
- DTMF Out-Of-Band and In-Band DTMF support
- Caller ID (limited to only Calling Number)
- Voice Mail access and interaction
- Early Media support
- Retrieval of a Parked Call
- Transferee in a Call Transfer
- Conference Call Participant
- Member of a Hunt group

Features Not Supported

- Caller ID Name presentation (Only the calling party number is displayed)
- Call Hold and Resume
- Call Forwarding on the device (Though forwarding can be configured on the PBX for the DN assigned to the endpoint)
- Call Waiting
- Initiating a Conference Call
- Initiating Attended Call Transfer
- Initiating Early Attended Call Transfer
- Initiating Blind Call Transfer
- Shared Line (configuration of shared line on device)
- Call Park (Initiating call park)
- Message Waiting Indicator

Known Issues and Limitations

When the Crestron Mercury phone is configured for Session Timer support, inbound calls cannot be answered. When the Session Timer is set to the default **Optional** setting on the Crestron Mercury and the Answer 200 OK is sent to the Avaya Aura, the Avaya CM adds a 2nd Session-Expires header. When this happens, the Avaya Aura does not send the ACK message for the 200 OK back to the Crestron Mercury, so the call is never answered. Disabling the Session Timer support on the Crestron Mercury allows the incoming call to be answered.

Crestron Mercury & Crestron Mercury X Configuration

Crestron Mercury - Power

The LAN port of the Crestron Mercury device needs to be connected to one PoE+ port to power it up for network connectivity with the Avaya Aura. The PoE switch should have LLDP functionality enabled for the device to power up and be completely functional. By default, the **POEPLUS** configuration is set to **OFF** on the device. In the tekVizion™ lab environment, the Crestron Mercury phones are powered by an AC line universal power pack.

Crestron Mercury X - Power

When using the Crestron Mercury X phone, an AC line universal power pack is needed to power the Crestron Mercury X.

AUX Port on Crestron Mercury X

The AUX Port is used on the Crestron Mercury X phone. When using the AUX Port on the Crestron Mercury X phone, the HD-RX-USB-2000-C converter box is needed in line with the Ethernet connection.

Discover/Access the Crestron Mercury

Crestron has a software tool available to discover and access the Crestron Mercury on the network: The Crestron Toolbox.

The Help menu on this tool assists the user through the discovery and configuration procedure.

The Crestron Mercury IP address, Host Name, MAC Address, Serial Number and Firmware Version can be viewed in the System info screen from the Home Screen by pressing and holding the Info link in the bottom left hand corner of the Crestron Mercury phone screen for 10 seconds.

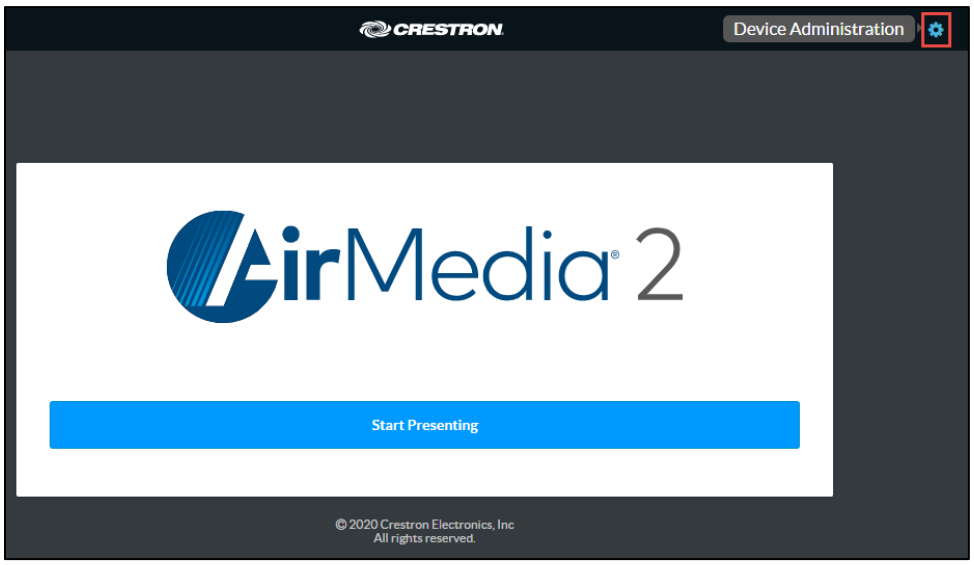
Crestron Mercury: System Info Screen

Crestron Mercury Web UI Sign In

Access the Crestron Mercury Web UI for the device by using an http session with the device's IP address. The initial page that displays is shown below.

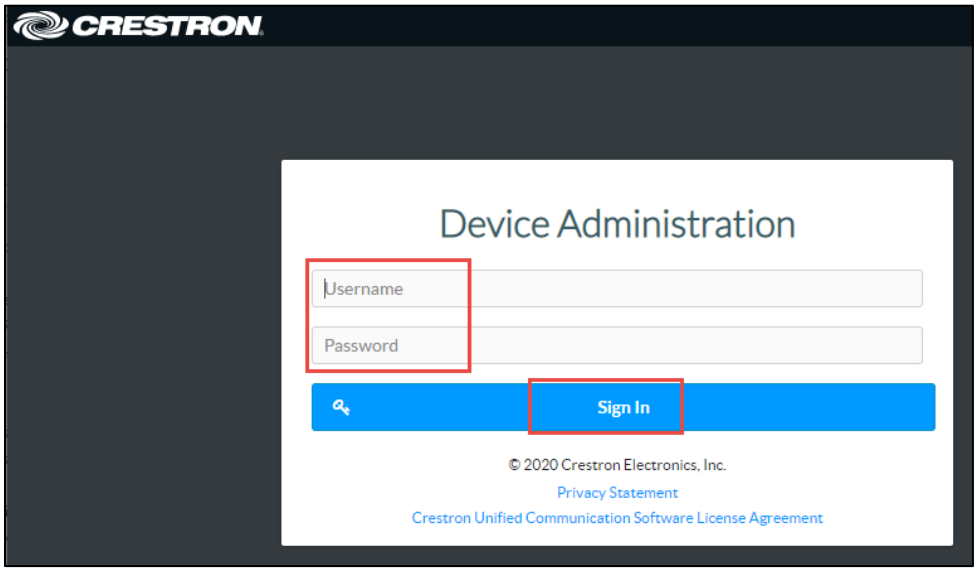
- Select the **Device Administration** link in top right corner.

Crestron Mercury: Device Administration



1. In the pop-up window provide **login credentials.**
2. Default Crestron Mercury Login credentials are **admin/admin**.
3. Click **Sign In.**

Crestron Mercury Web UI: Sign In



Crestron Mercury

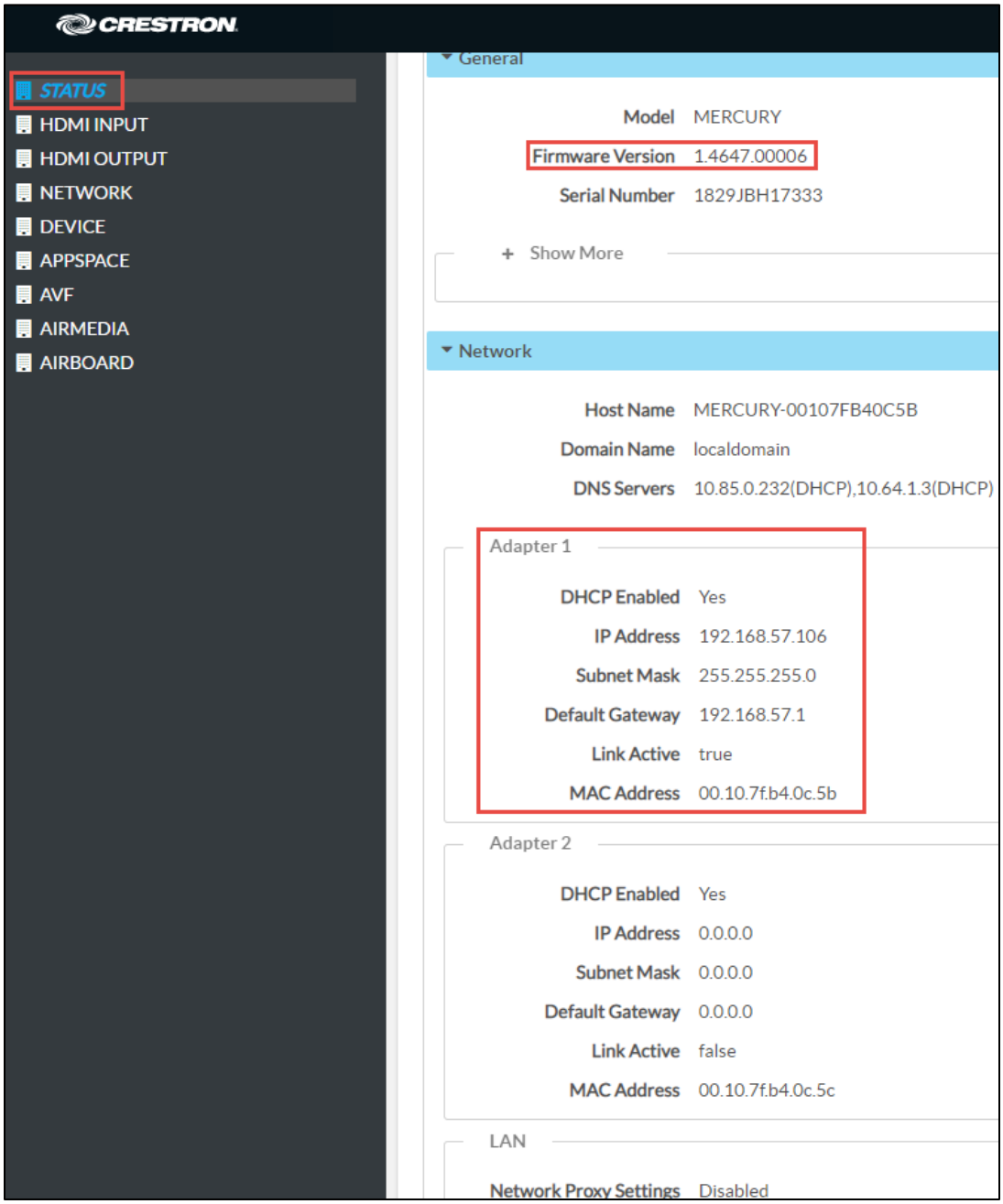
In the tekVizion lab environment, one DUT used is a Crestron Mercury phone with the Ethernet cable connected to the LAN port of the Crestron Mercury. Configuration for this setup is shown below.

Status

The **Status** screen shown below displays basic device information:

- The **Firmware Version** and **Network** info of the Crestron Mercury are shown here.

Crestron Mercury: Status



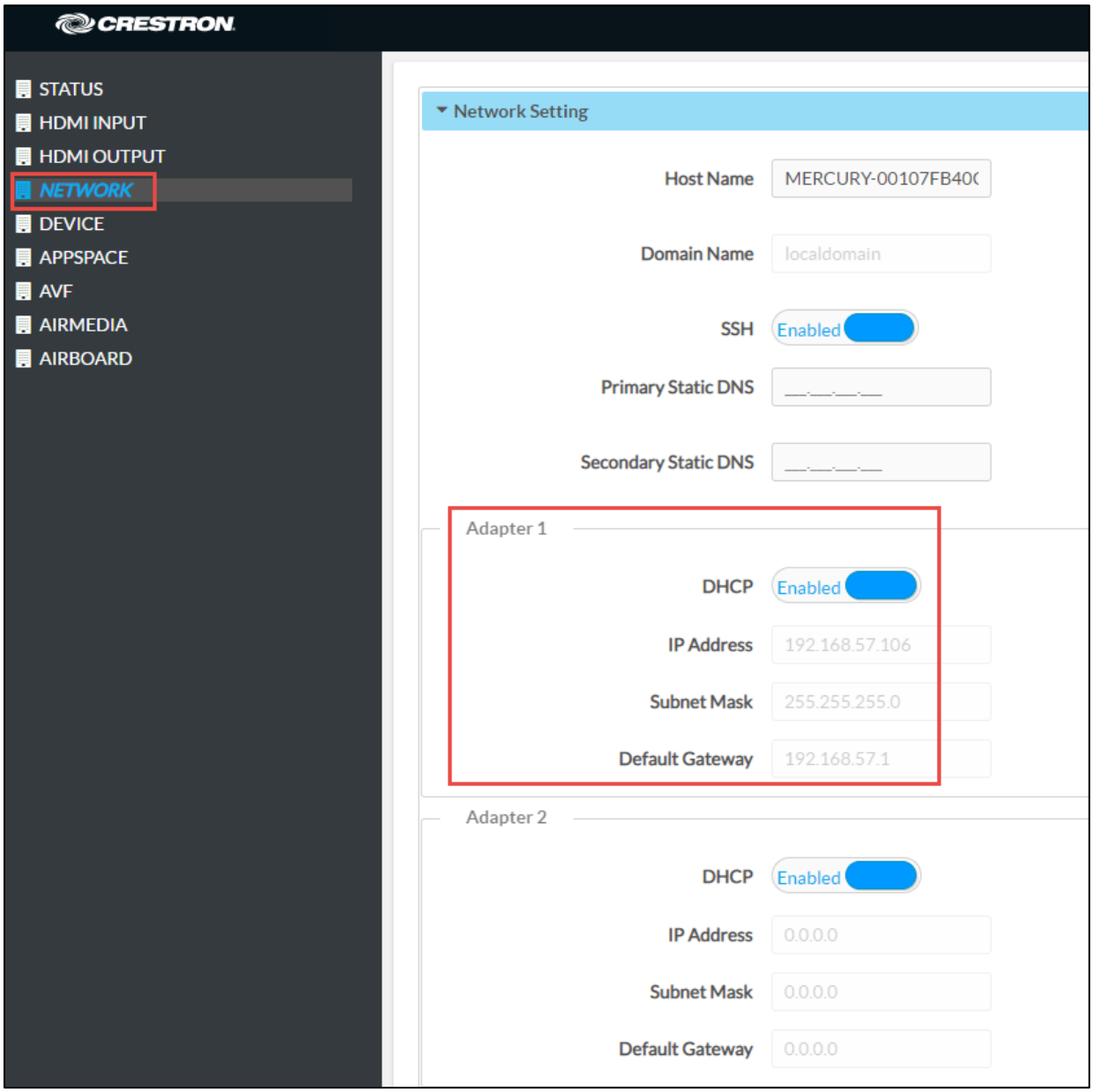
Network Configuration

The Crestron Mercury Network settings can be configured from the Network page.

On the Crestron Mercury Web UI, navigate to **Network.**

1. **DHCP:** The Crestron Mercury is configured as DHCP.
2. The LAN Port is used on the Crestron Mercury, so **Adapter 1** is configured via DHCP.
3. Click **Save Changes.**

Crestron Mercury: Network: DHCP



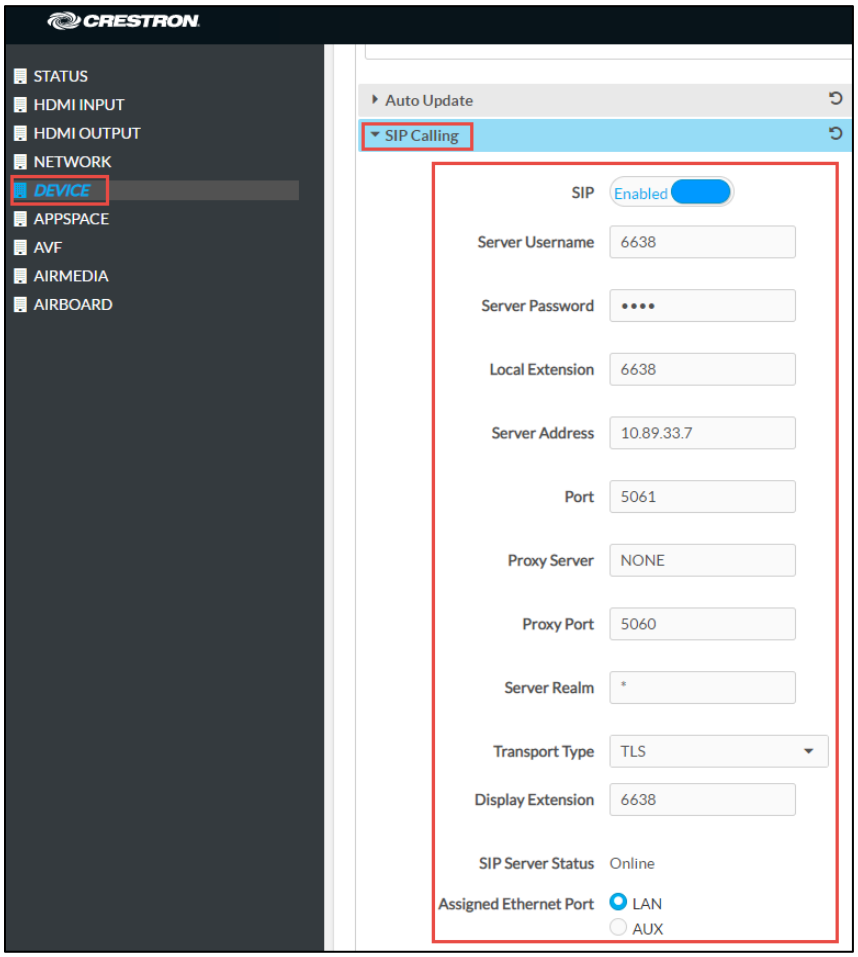
SIP Calling Parameters

Configure the Crestron Mercury SIP Parameters to enable Crestron Mercury communication with the Avaya Aura SM.

From the Crestron Mercury Web UI, navigate to **Device → SIP Calling.**

1. **SIP**: click the box to display **Enabled.**
2. **Server Username**: Enter the end user configured on the Avaya Aura CM for this device, (**6638**).
3. **Server Password**: User's password as configured on the Avaya Aura CM.
4. **Local Extension**: Enter the directory number configured for this device on the Avaya Aura, (**6638**).
5. **Server Address**: Enter the IP address of the Avaya Aura SM, (**10.89.33.7**).
6. **Server Port**: For the TLS Secure setup, port **5061** is used.
7. **Transport Type**: For the TLS Secure setup, **TLS** Transport is used.
8. **Display Extension**: **6638** is used.
9. **Assigned Ethernet Port** is set to **LAN.**
10. Click **Save Changes.**
11. **SIP Server Status** shows **Online** when successfully registered to the PBX.

Crestron Mercury: Device: SIP Calling



Crestron Mercury X

In the tekVizion lab environment, one DUT is a Crestron Mercury X phone with the Ethernet cable connected to the AUX port. The Crestron HD-RX-USB-2000-C converter box is needed in-line with the Ethernet connection when the AUX port is used. The specific Crestron Mercury X configuration for this setup is shown below, the rest of the configuration is the same as the above Crestron Mercury configuration.

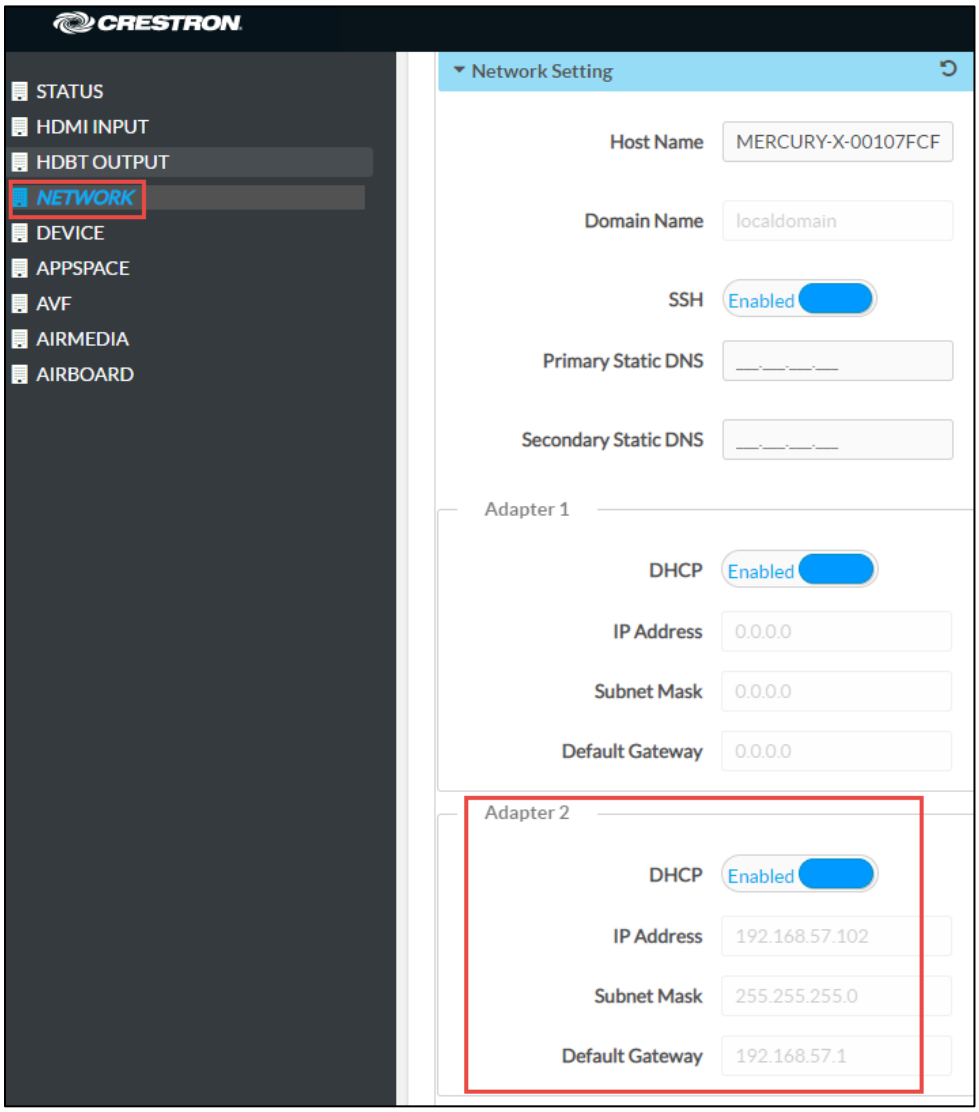
Network Configuration

The Crestron Mercury Network settings can be configured from the Network page.

On the Crestron Mercury Web UI, navigate to **Network.**

1. **DHCP:** The Crestron Mercury is configured as DHCP. The AUX Port is used on the Crestron Mercury X, so **Adapter 2** is configured as **DHCP.**
2. Click **Save Changes.**

Crestron Mercury X: Network



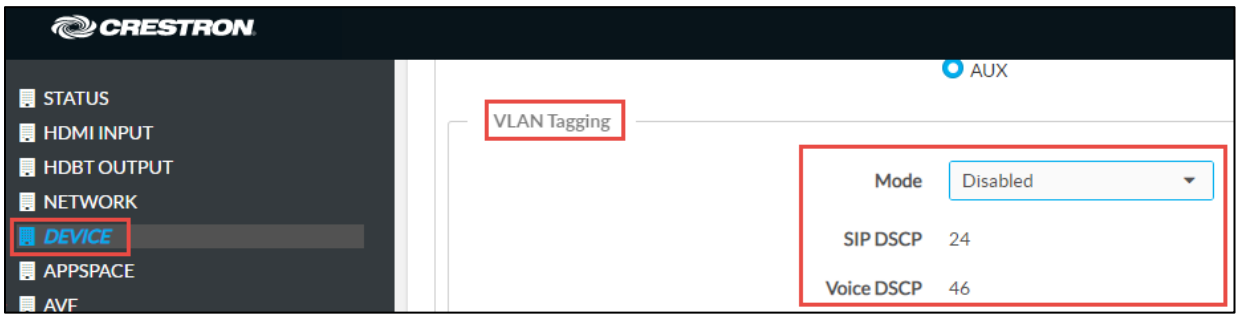
VLAN Tagging

VLAN Tagging on the Crestron Mercury allows you to assign DSCP values to the SIP and Media messages. It also allows you to assign a Priority value to the VLAN used for the SIP and Media messages. When enabled, VLAN Tagging uses a 2nd IP address that is assigned to the Crestron Mercury phone for the SIP and Media messages. The IP address is assigned by a Local Network Cisco switch (Cisco SG350-28P), providing the VLAN Tagging configuration info to the Crestron Mercury.

The available **VLAN Tagging Mode** settings are shown below: From the Crestron Mercury Web UI, navigate to **Device → SIP Calling.**

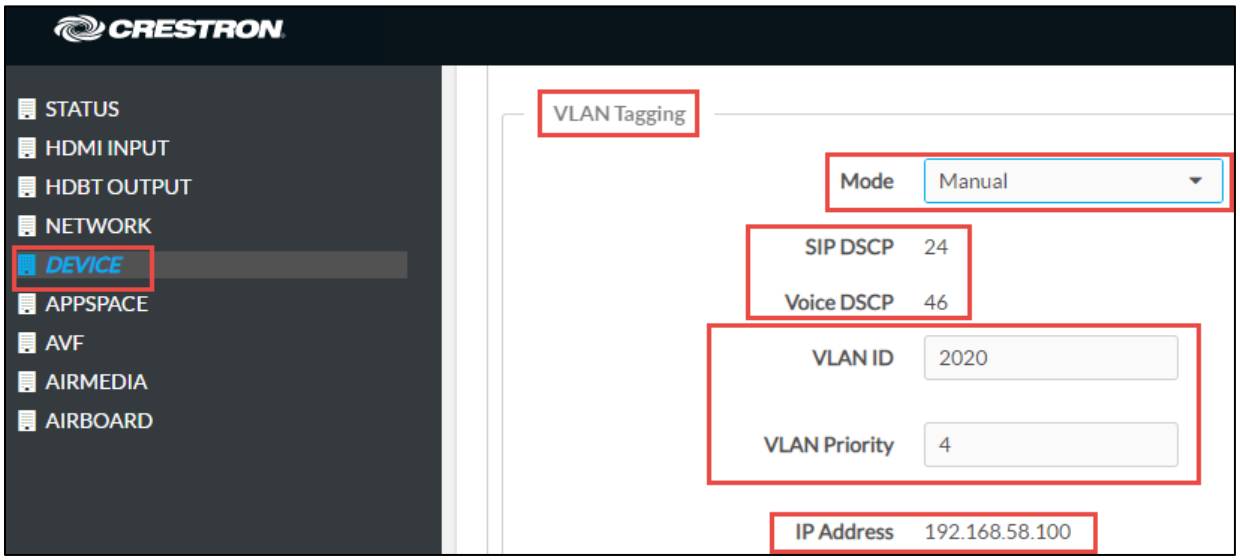
1. **Disabled** – Uses just 1 IP address for the Data IP address SIP and Media. The default DSCP value assigned to SIP is **24** and to Media is **46**. The Priority VLAN value is not assigned to the Messages. The default Crestron Mercury setting is **Disabled**.

Crestron Mercury: Device: SIP Calling: VLAN Tagging - Disabled



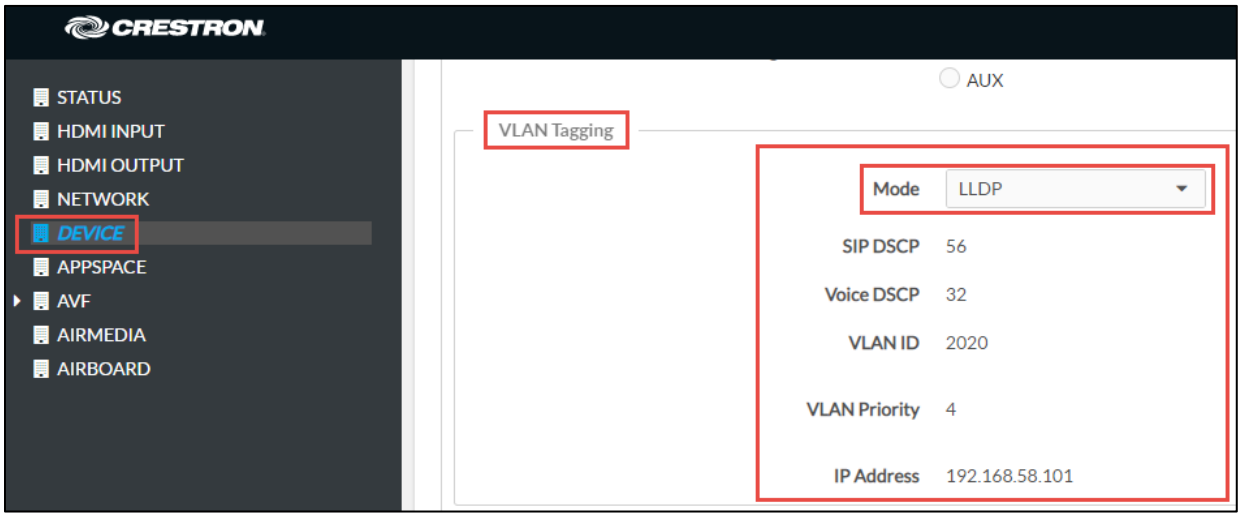
2. **Manual** – Allows you to assign the VLAN ID and VLAN priority to be used by the Crestron Mercury. The default DSCP values (**SIP – 24** and **Voice – 46**) are assigned. The 2nd IP address, used for SIP and Media is assigned to the Crestron Mercury by the local network switch with the VLAN Tagging configuration.

Crestron Mercury: Device: SIP Calling: VLAN Tagging - Manual



3. **LLDP** – Pulls the VLAN Tagging information from the local network switch with the VLAN Tagging configuration. **The SIP End Point test plan was executed with this setting.**

Crestron Mercury: Device: SIP Calling: VLAN Tagging - LLDP



VLAN Tagging Local Network Switch – Cisco SG350-28P

The tekVizion lab environment used a Cisco SG350-28P switch to provide the 2nd IP address used for SIP & Media, and the VLAN Tagging configuration for the Crestron Mercury and Crestron Mercury X phone when **LLDP** is set as the **Mode** for the Crestron Mercury.

The Crestron Mercury phones are connected directly to the Cisco SG350-28P switch in the lab setup.

The Running Configuration for the VLAN Tagging switch is provided below. The following configuration settings are used in the tekVizion lab VLAN Tagging environment.

1. **Voice Vlan ID 2020**
2. **LLDP Med Network-Policy**
   - 3 voice-signaling vlan 2020 vlan-type tagged up 4
   - 4 voice vlan 2020 vlan-type tagged up 4 dscp 32
   - 9 voice-signaling vlan 2020 vlan-type tagged up 4 dscp 32
   - 10 voice vlan 2020 vlan-type tagged up 4 dscp 32
   - 15 voice-signaling vlan 2020 vlan-type tagged up 4 dscp 56
   - 16 voice vlan 2020 vlan-type tagged up 4 dscp 32
3. **Interface Port 4 - Crestron Mercury phone**
   - interface GigabitEthernet4
   - description Crestron Mercury2
   - switchport mode trunk
   - lldp med network-policy add 15
   - lldp med network-policy add 16
4. **Interface Port 7 - Crestron Mercury phone**
   - interface GigabitEthernet7
   - description Crestron Mercury 5
   - switchport mode trunk
   - lldp med network-policy add 15
   - lldp med network-policy add 16

Cisco SG350_28P – Running Configuration

```
switch94214e#show run
config-file-header
switch94214e
v2.4.5.71 / RTESLA2.4.5_930_181_144
CLI v1.0
file SSD indicator encrypted
@
ssd-control-start
ssd config
ssd file passphrase control unrestricted
no ssd file integrity control
ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0
!
!
unit-type-control-start
unit-type unit 1 network gi uplink none
unit-type-control-end
!
vlan database
vlan 2,10-11,15,200,2018-2020,4030
exit
voice vlan id 2020
voice vlan oui-table add 0001e3 Siemens_AG_phone________
voice vlan oui-table add 00036b Cisco_phone______________
voice vlan oui-table add 00096e Avaya_____________________
voice vlan oui-table add 000fe2 H3C_Aolynk_______________
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone
voice vlan oui-table add 00d01e Pingtel_phone___________
voice vlan oui-table add 00e075 Polycom/Veritel_phone___
voice vlan oui-table add 00e0bb 3Com_phone______________
no lldp med network-policy voice auto

lldp med network-policy 3 voice-signaling vlan 2020 vlan-type tagged up 4
lldp med network-policy 4 voice vlan 2020 vlan-type tagged up 4 dscp 32
```

```
lldp med network-policy 9 voice-signaling vlan 2020 vlan-type tagged up 4 dscp 32
lldp med network-policy 10 voice vlan 2020 vlan-type tagged up 4 dscp 32

lldp med network-policy 15 voice-signaling vlan 2020 vlan-type tagged up 4 dscp 56
lldp med network-policy 16 voice vlan 2020 vlan-type tagged up 4 dscp 32

link-flap prevention disable
bonjour interface range vlan 1
hostname switch94214e
no passwords complexity enable
ip ssh server
ip telnet server
!
interface vlan 2
 name Data
!
interface vlan 15
 name "RSPAN VLAN"
 remote-span
!
interface GigabitEthernet1
 description PoE1
 storm-control broadcast level 10
 storm-control multicast level 10
 port security max 10
 port security mode max-addresses
 port security discard trap 60
 spanning-tree portfast
 spanning-tree bpduguard enable
 switchport mode trunk
 switchport trunk allowed vlan remove 2-2019,2021-4094
 macro description "ip_phone_desktop_1 | no_ip_phone_desktop |
ip_phone_desktop"
 no macro auto smartport
 macro auto smartport type ip_phone_desktop
!
```

```
interface GigabitEthernet2
 description PoE2
 storm-control broadcast level 10
 storm-control multicast level 10
 port security max 10
 port security mode max-addresses
 port security discard trap 60
 spanning-tree portfast
 spanning-tree bpduguard enable
 switchport mode trunk
 switchport trunk allowed vlan remove 2-2019,2021-4094
 macro description "ip_phone_desktop_2 | no_ip_phone_desktop |
ip_phone_desktop"
 macro auto smartport type ip_phone_desktop
!
interface GigabitEthernet3
 description Crestron Mercury1
 switchport mode trunk
 lldp med network-policy add 15
 lldp med network-policy add 16
!
interface GigabitEthernet4
 description Crestron Mercury2
 switchport mode trunk
 lldp med network-policy add 15
 lldp med network-policy add 16
!
interface GigabitEthernet5
 shutdown
 description Crestron Mercury3
 switchport mode trunk
!
interface GigabitEthernet6
 description Crestron Mercury4
 switchport mode trunk
 lldp med network-policy add 3
```

```
 lldp med network-policy add 4
!
interface GigabitEthernet7
 description Crestron Mercury5
 switchport mode trunk
 lldp med network-policy add 15
 lldp med network-policy add 16
!
interface GigabitEthernet13
 description PoE3
 storm-control broadcast level 10
 storm-control multicast level 10
 port security max 10
 port security mode max-addresses
 port security discard trap 60
 spanning-tree portfast
 spanning-tree bpduguard enable
 switchport mode trunk
 switchport trunk allowed vlan remove 2-2019,2021-4094
 macro description "ip_phone_desktop_3 | no_ip_phone_desktop |
ip_phone_desktop"
 macro auto smartport type ip_phone_desktop
!
interface GigabitEthernet14
 description PoE4
 storm-control broadcast level 10
 storm-control multicast level 10
 port security max 10
 port security mode max-addresses
 port security discard trap 60
 spanning-tree portfast
 spanning-tree bpduguard enable
 switchport mode trunk
 switchport trunk allowed vlan remove 2-2019,2021-4094
 macro description "ip_phone_desktop_4 | no_ip_phone_desktop |
ip_phone_desktop"
 !next command is internal.
```

```
 macro auto smartport dynamic_type ip_phone_desktop
!
interface GigabitEthernet24
 description Wireshark
 bridge multicast unregistered filtering
 switchport trunk native vlan none
 ip igmp version 2
 ip igmp query-interval 60
!
interface GigabitEthernet25
 description DHCP
 spanning-tree link-type point-to-point
 switchport mode trunk
 macro description switch
!
interface GigabitEthernet26
 shutdown
 description dhcp1
 spanning-tree link-type point-to-point
 switchport mode trunk
!
exit
monitor session 1 destination remote vlan 15 reflector-port GigabitEthernet24 network
monitor session 1 source interface GigabitEthernet4 both
monitor session 1 source interface GigabitEthernet7 both
monitor session 1 source interface GigabitEthernet13 both
monitor session 1 source interface GigabitEthernet14 both
```

Crestron Mercury & Crestron Mercury X - Session Timer Support

To answer an inbound call to the Crestron Mercury phones, Session Timer support on the Crestron Mercury phone needs to be disabled by setting the CLI Session Timer to **INACTIVE.** The Crestron Mercury & Crestron Mercury X default Session Timer setting is **OPTIONAL**.

When the Session Timer is supported on the Crestron Mercury and the answer **200 OK** is sent to the Avaya Aura, the Avaya CM adds a 2nd Session-Expires header. This prevents the Avaya Aura from sending the ACK message for the 200 OK back to the Crestron Mercury, and the call is never answered.

SipSessionTimer Inactive

Sipsessiontimer inactive command is used to disable the Session Timer support. The Session Timer setting can be view with the **Sipstate** command.

Crestron Mercury X: CLI: Session Timer Support

```
MERCURY-X>sipsessiontimer inactive
Success: New parameter has been set

MERCURY-X>sipstate

Current SIP States
------------------------------
Server registered   = TRUE
Door station mode   = FALSE
Call in progress    = FALSE
Call hold           = FALSE
Push-To_Talk        = FALSE
Do not disturb      = FALSE
Video started       = FALSE
Video blocked       = FALSE
Video can show      = FALSE
Default ringer      = TRUE
Ring state          = FALSE
Ringback state      = FALSE
Group call flag     = FALSE
User Mute state     = FALSE
Local Mute state    = FALSE
Multicast flag      = FALSE
Support answer      = FALSE
Request auto        = FALSE
Request urgent      = FALSE
RFC 2833 support    = TRUE
Call timeout        = 120 (secs)
Answer timeout      = 0 (secs)
Rewrite CONTACT     = TRUE
Rewrite SDP         = FALSE
Rewrite VIA         = TRUE
Voice-AutoListen    = FALSE
Sound device        = not active
SIP DSCP codepoint  = 56
RTP DSCP codepoint  = 32
Verify server       = TRUE
Verify client       = FALSE
SRTP                = mandatory
Session Timer       = inactive
Early Media         = auto
Video Enable        = auto
Invite Response     = 183
Interface           = AUX_SIPVLAN
Reg Timeout         = 300
```

Crestron Mercury & Crestron Mercury X - RFC 2833 Support

To configure the RFC 2833 support on the Crestron Mercury, the **Sipaudiomode RFC2833** command is used from the Crestron Mercury CLI and accessed from the Crestron Toolbox. There are 2 options: **ON** or **OFF**.

1. **ON** (TRUE): Considered Out-of-band, RTP DTMF Events are viewable in the RTP stream. This is the Default setting.
2. **OFF** (FALSE): Considered In-band, RTP DTMF Events are not viewable in the RTP Stream.

The RFC 2833 Support setting **TRUE** is used for most of the testing. Two Specific DTMF test cases are used with both settings: Call to an IVR and Call to the Avaya Communication Manager Messaging voice mail system, where the DTMF digits are recognized.

SipAudioMode RFC2833 On

Sipaudiomode RFC2833 on command is used to enable RFC2833 Out-of-band support. The RFC2833 setting can be viewed from the **Sipstate** command.

Crestron Mercury X: CLI: RFC 2833 Support

```
MERCURY-X>sipaudiomode rfc2833 on
RFC2833 support has been turned on.


MERCURY-X>sipstate

Current SIP States
------------------------------
Server registered   = TRUE
Door station mode   = FALSE
Call in progress    = FALSE
Call hold           = FALSE
Push-To_Talk        = FALSE
Do not disturb      = FALSE
Video started       = FALSE
Video blocked       = FALSE
Video can show      = FALSE
Default ringer      = TRUE
Ring state          = FALSE
Ringback state      = FALSE
Group call flag     = FALSE
User Mute state     = FALSE
Local Mute state    = FALSE
Multicast flag      = FALSE
Support answer      = FALSE
Request auto        = FALSE
Request urgent      = FALSE
RFC 2833 support    = TRUE
Call timeout        = 120 (secs)
Answer timeout      = 0 (secs)
Rewrite CONTACT     = TRUE
Rewrite SDP         = FALSE
Rewrite VIA         = TRUE
Voice-AutoListen    = FALSE
Sound device        = not active
SIP DSCP codepoint  = 56
RTP DSCP codepoint  = 32
Verify server       = TRUE
Verify client       = FALSE
SRTP                = mandatory
Session Timer       = inactive
Early Media         = auto
Video Enable        = auto
Invite Response     = 183
Interface           = AUX_SIPVLAN
Reg Timeout         = 300
```

Crestron Mercury & Crestron Mercury X - SIP Interface Port

To configure the Crestron Mercury X Assigned Ethernet Port to use the LAN or RX OUT Ethernet ports, use the SIPINTERFACE CLI command. When the HD-RX-USB-2000-C Receiver is connected to the Crestron Mercury X, the **AUX** (RX OUT) port is used.

The **Assigned Ethernet Port** can also be configured from the Crestron Mercury Web UI, in the **SIP Calling** section.

SipInterFace AUX

Sipinterface AUX is used in the Crestron Mercury X CLI to activate the RX OUT Ethernet port as the SIP Interface port to be used. Using the RX OUT Ethernet port allows the internet connection to be routed through the HD-RX-USB-2000-C receiver and then connected to the RX OUT port on the Crestron Mercury X.

Crestron Mercury X: CLI: SIPINTERFACE Support

```
MERCURY-X>sipinterface aux
Success: New SIP interface has been set.


MERCURY-X>sipinfo
SIP Parameters
------------------------------
SIP: ENABLED
------------------------------
SIP audio mode: FD
SIP auto mode: NONE
SIP local ext: 6637
SIP local name: CRESTRON
SIP local port: 5060
SIP connection mode: SERVER
SIP page group(s): CRESTRON
SIP realm: *
SIP remote config file: NONE
SIP server name: NONE
SIP server port: 5061
SIP server ip address: 10.89.33.7
SIP server username: 6637
SIP server password: ****
SIP Name server: NONE
SIP proxy server: NONE:5060
SIP STUN server: NONE
SIP STUN domain: NONE
SIP multicast address: 227.1.1.1
SIP multicast port: 1234
SIP transport type: TLS
SIP protocol qos: 24
SIP media port: 40000
SIP rtp qos: 46
SIP session timer: inactive
SIP Interface: AUX
SIP registration timeout: 300
```

Crestron Mercury & Crestron Mercury X Secure RTP (SRTP)

The Default Crestron Mercury RTP setting is Mandatory if TLS Transport is used.

SipSettings SRTP

To configure the SRTP settings on the Crestron Mercury, the **Sipsettings SRTP** command is used from the Crestron Mercury CLI accessed from the Crestron Toolbox. There are 3 options used with the **Sipsettings SRTP** command: **0** (Disabled), **1** (Optional) and **2** (Mandatory). The default setting is **Mandatory**.

1. 0=Disabled: Non-Secure RTP.
2. 1=Optional: 1st priority is Non-Secure RTP but secures the RTP if SRTP is offered to the Crestron Mercury.
3. 2=Mandatory: Secure RTP (SRTP).

The SRTP setting can be viewed from the **Sipstate** command.

Crestron Mercury: CLI: Sipsettings SRTP

```
MERCURY-X>sipstate

Current SIP States
------------------------------
Server registered   = TRUE
Door station mode   = FALSE
Call in progress    = FALSE
Call hold           = FALSE
Push-To_Talk        = FALSE
Do not disturb      = FALSE
Video started       = FALSE
Video blocked       = FALSE
Video can show      = FALSE
Default ringer      = TRUE
Ring state          = FALSE
Ringback state      = FALSE
Group call flag     = FALSE
User Mute state     = FALSE
Local Mute state    = FALSE
Multicast flag      = FALSE
Support answer      = FALSE
Request auto        = FALSE
Request urgent      = FALSE
RFC 2833 support    = TRUE
Call timeout        = 120 (secs)
Answer timeout      = 0 (secs)
Rewrite CONTACT     = TRUE
Rewrite SDP         = FALSE
Rewrite VIA         = TRUE
Voice-AutoListen    = FALSE
Sound device        = not active
SIP DSCP codepoint  = 56
RTP DSCP codepoint  = 32
Verify server       = TRUE
Verify client       = FALSE
SRTP                = mandatory
Session Timer       = inactive
Early Media         = auto
Video Enable        = auto
Invite Response     = 183
Interface           = AUX_SIPVLAN
Reg Timeout         = 300

You have 0 active call
```

Certificates

For a successful TLS handshake with the Avaya Aura Session Manager, the Crestron Mercury needs a root certificate – *root.cer.*

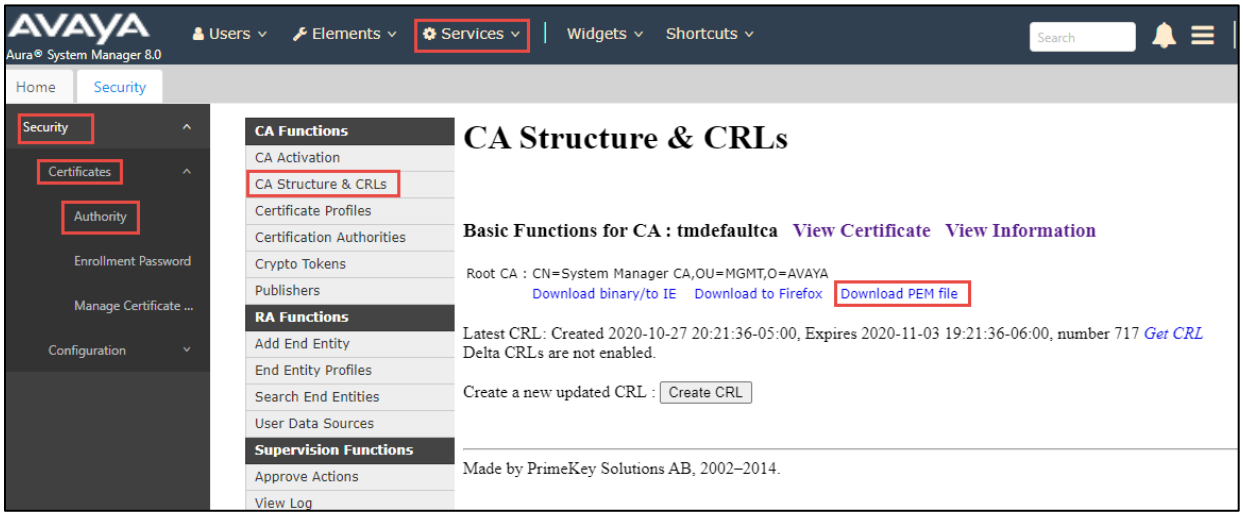
This is the certificate that is downloaded from the certificate authority that serves the Avaya Aura Session Manager (local Avaya CA). This certificate is required by the Crestron Mercury to allow the device to validate the Avaya Aura Session Manager when the **Enable Server Validation** is enabled in the **SIP Calling** configuration screen shown above.

Avaya Aura Root Certificate

The Avaya Aura Root Certificate needs to be downloaded to your workstation. To Download Avaya Aura CA from Avaya Aura System Manager:

1. Navigate to the **Services** column and select **Security.**
2. Click on the **Certificates** dropdown and select **Authority.**
3. Click **CA Structure & CRLs.**
4. Click **Download PEM file.**
5. Save the file on your computer as **systemmanager80.cer** (used in this example).

Avaya Aura System Manager: Download Root Certificate



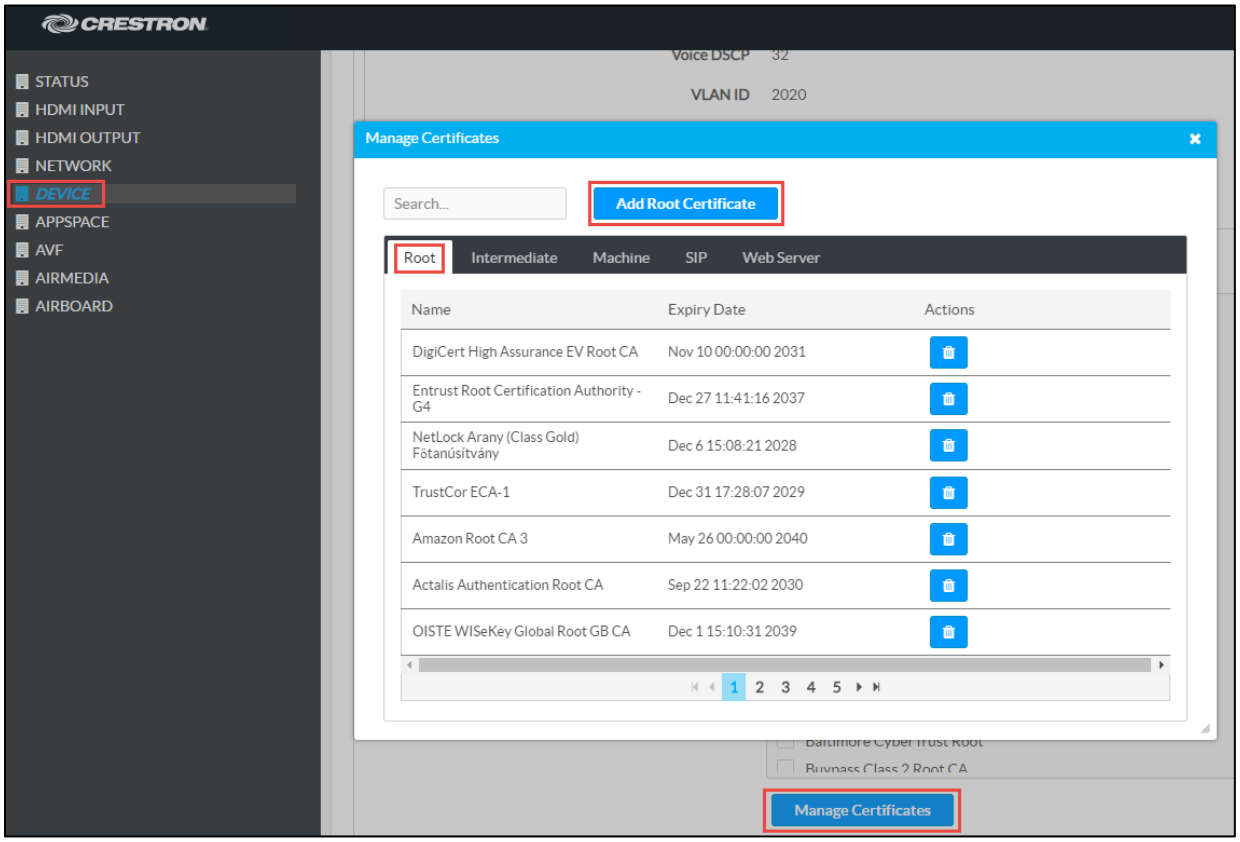
Adding Root Certificate to the Crestron Mercury

To upload certificates to the Crestron Mercury:

Navigate to **Device-> SIP Calling.**

1. Click on **Manage Certificates.**
2. In pop-up window, click on **Add Root Certificate.**

Crestron Mercury: Device: SIP Calling: Manage Certificate

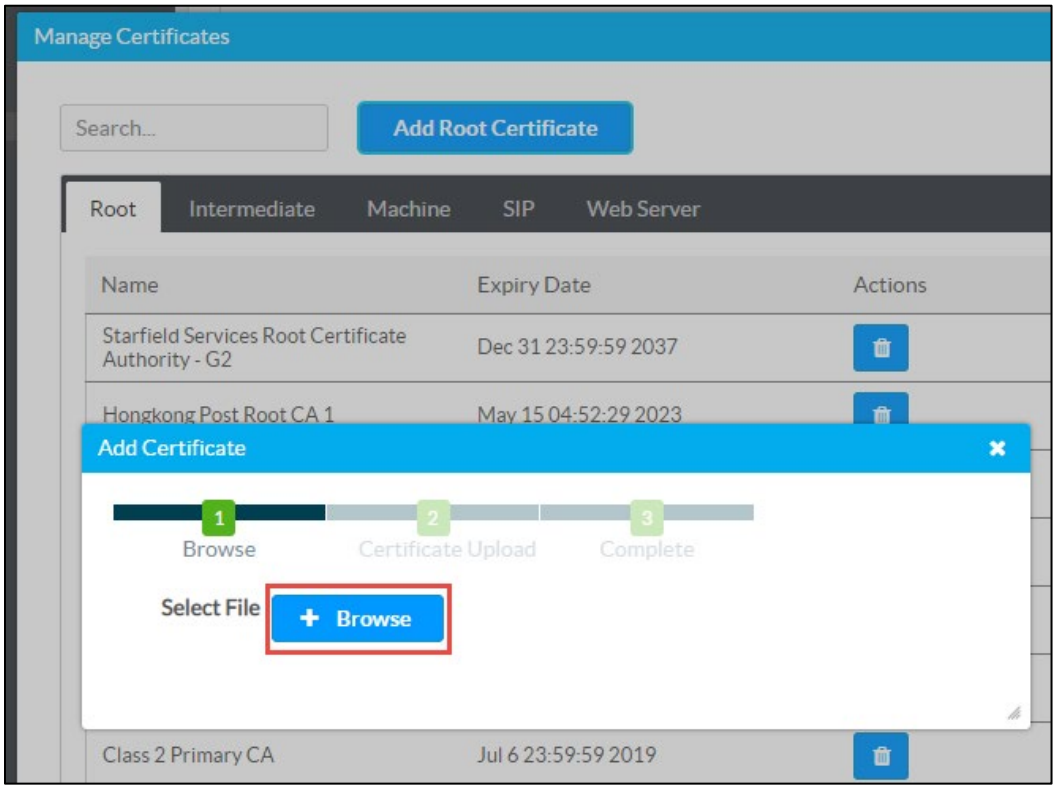


Add Certificate

In the Add Certificate pop-up window, browse to the location of the Root Certificate downloaded from the Avaya Aura SM.

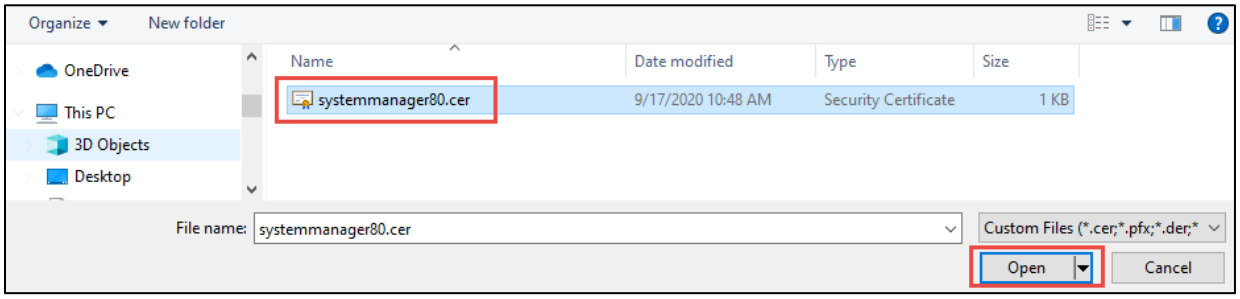
- In the **Add Certificate** pop-up window, click the **+ Browse** button.

Crestron Mercury: Manage Certificates: Add Certificate



1. In the pop-up window, select the – root_cer.cer file saved on your computer (**systemmanagerca80.cer** in this example).
2. Click **Open.**

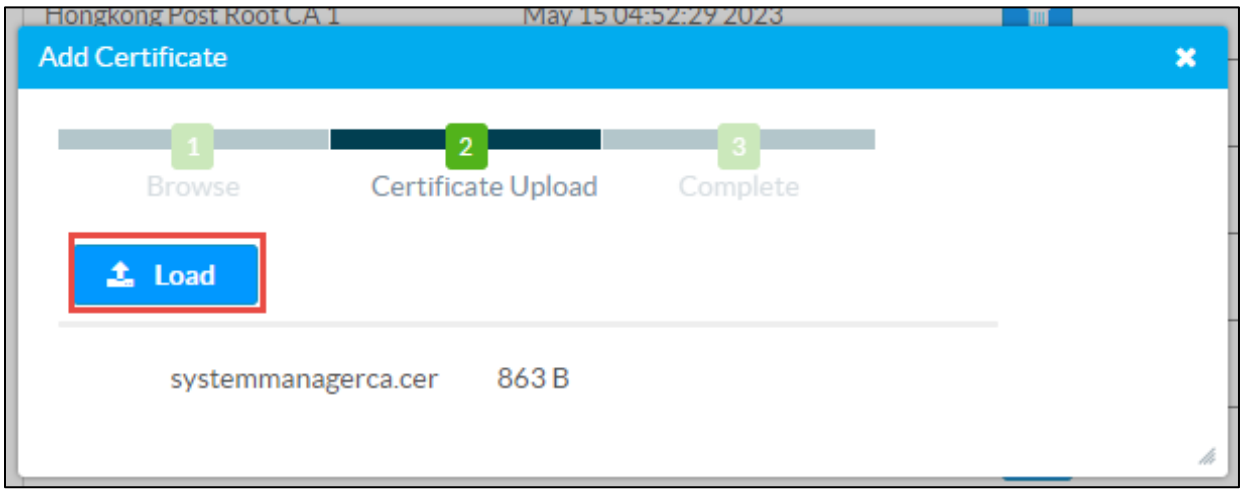
Crestron Mercury: Add Certificate: Select Certificate



Load Certificate

- Click the **Load** button to upload Root Certificate to the Crestron Mercury.

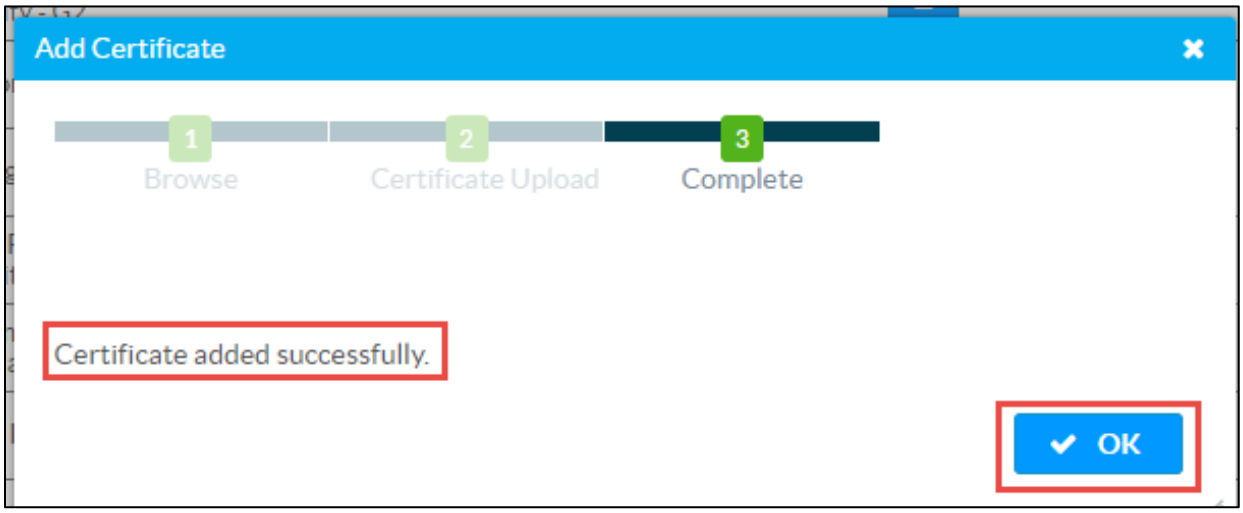
Crestron Mercury: Add Certificate: Load Certificate



Upload Successful

- Click the **OK** button after the Certificate is added successfully.

Crestron Mercury: Add Certificate: Certificate added successfully

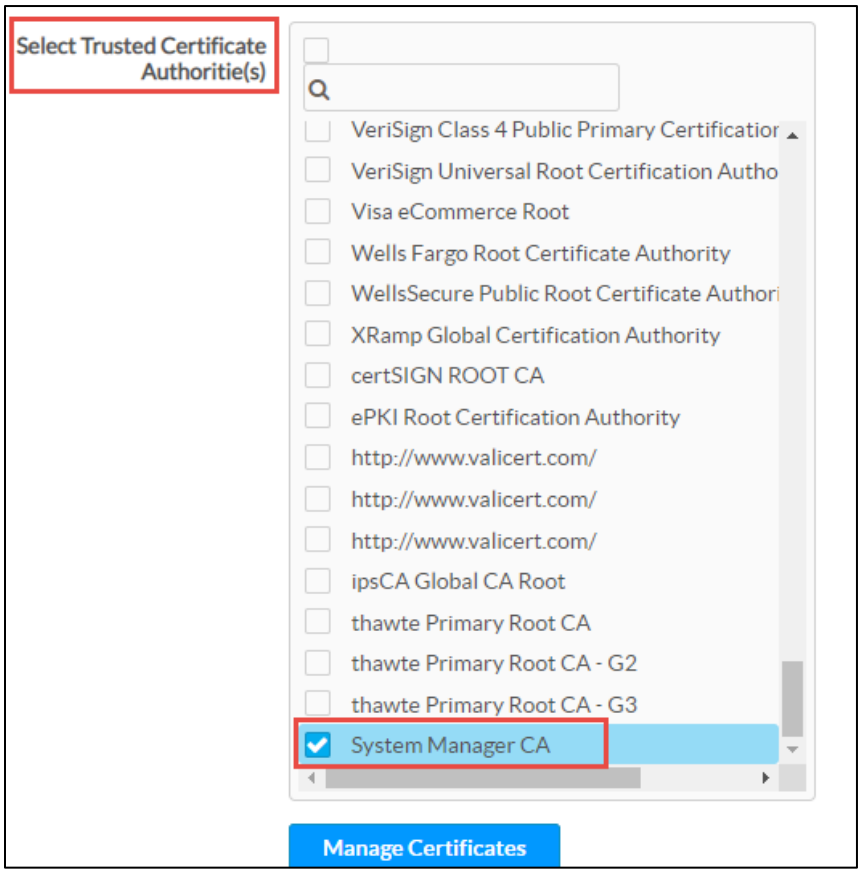


Select Trusted Certificate Authorities

Once the upload is complete, the Root Certificate may not show up in the Select Trusted Certificate Authoritie(s) section until the page is refreshed. If this occurs, refresh the web page and Navigate back to **Device -> SIP Calling**. The newly added root-cer certificate should appear in the list of trusted certificate authoritie(s).

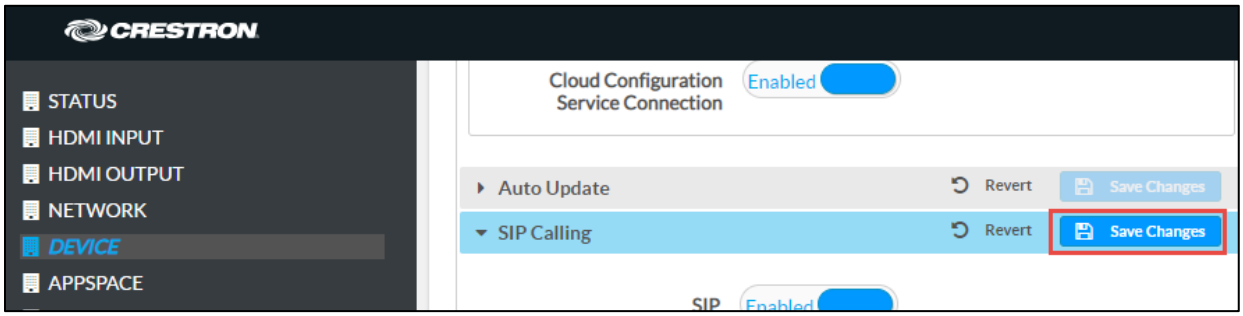
- Select the **System Manager CA** Root Certificate.

Crestron Mercury: Add Certificate: Select Trusted Certificate Authoritie(s)



- Click the **Save Changes** button at the top of the **SIP Calling** section.

Crestron Mercury: Add Certificate: Save Changes

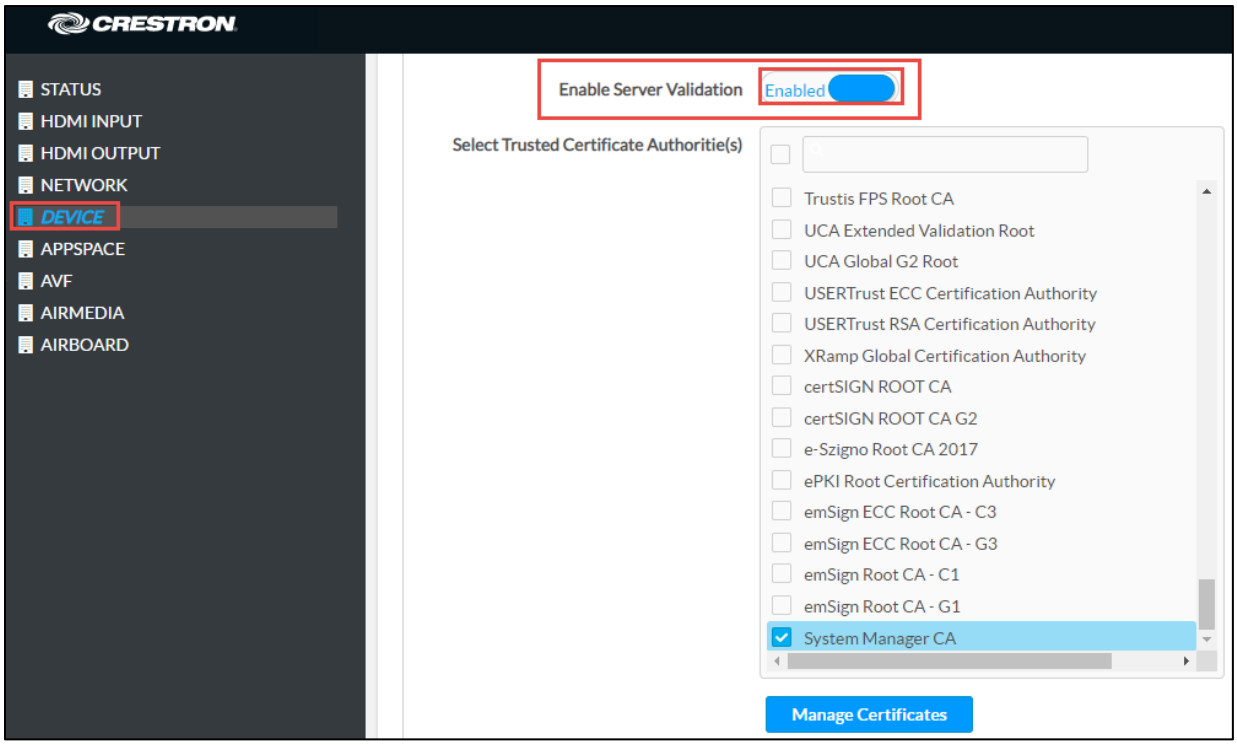


Enable Server Validation

If the TLS Handshake between the Crestron Mercury phone and the Avaya Aura is not successful after the Root Certificate has been added to the Crestron Mercury, it may be necessary to **Disable** the **Enable Server Validation**. In the tekVizion lab environment, the TLS Handshake between the Crestron Mercury and the Avaya Aura is successful with the **Enable Server Validation** set as **Enabled** or **Disabled**.

- From the Crestron Mercury Web UI, navigate to **Device → SIP Calling.**

Crestron Mercury: Device: SIP Calling



Avaya Aura Communication Manager Configuration

This section describes the configuration necessary on the Avaya Aura Communication Manager (Avaya CM) to integrate the Crestron Mercury in secure mode.

NOTE: It is assumed that the general installation and basic Avaya Aura configuration have already been administered.

Node Names

Configure the node IP for Avaya Aura Session Manager and Avaya CM.

Use the **change node-names ip** command to add the **node name**. In this example, **procr and Lab133-SM80** have been added with their respective IPs.

1. **Lab133-SM80** is the Avaya Aura Session Manager used in this example to register SIP phones and third-party SIP devices.
2. **procr** is used to register SIP trunk between Avaya CM and Avaya SM.

Avaya Aura CM: Configuration Node

```
10.89.33.4 - PuTTY
change node-names ip                                          Page   1 of   2
                                IP NODE NAMES
    Name                IP Address
Lab133-SM80           10.89.33.7
Lab133-SM81           10.89.33.207
VFNL                  62.140.143.225
acmm                  10.89.26.25
default               0.0.0.0
gateway               10.89.33.1
procr                 10.89.33.4
procr6                ::

( 8  of 8    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Dial Plan analysis

Several dial strings are configured to allow calling between stations, calling to PSTN and accessing PBX features.

Configure the following dial patterns using the **change dialplan analysis** command.

1. Dialed string: **5000**, used in this example for Voice Mail number.
2. Dialed string: **66**, used in this example for station number.
3. Dialed string: **8**, used in this example as feature access code.
4. Dialed string: **9**, used in this example as feature access code.
5. Dialed string: *****, used in this example as feature access code.
6. Dialed string: **#**, used in this example as a dial access code.

The **display dialplan analysis** command can be used to view the configured dialed strings/codes.

Avaya Aura CM: Dial Plan Analysis

```
display dialplan analysis                                    Page   1 of  12
                           DIAL PLAN ANALYSIS TABLE
                                 Location: all            Percent Full: 3

   Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
   String   Length Type     String   Length Type     String   Length Type
 0            10 ext      *            4  fac
 0432072658   10 ext      #            4  dac
 09            4  ext
 2             4  ext
 21            7  ext
 2555          4  udp
 3             4  ext
 5000          4  ext
 598           7  ext
 66            4  ext
 7             5  ext
 75            4  ext
 78            4  udp
 8             1  fac
 9             1  fac

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

IP-Network-Region

All the SIP phones used are configured in **ip-network-region 2**. **Domain** name. **Codec Set** parameters are configured as in example below.

1. **Domain**: set as **lab.tekvizion.com.**
2. **Codec Set:** IP-Codect-set **2**.

Avaya Aura CM: IP-network-region

```
display ip-network-region 2                                     Page   1 of  20
                              IP NETWORK REGION
  Region: 2       NR Group: 2
Location: 1       Authoritative Domain: lab.tekvizion.com
    Name: VodafonePSTN          Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the PBX and PSTN.

In the tekVizion lab environment, **ip-codec-set 2** is used for this purpose. The Crestron Mercury supports **G.711A**, **G.711MU, G.729 and G.722**.

1. The following codecs are included in this codec set, enter **G.711MU, G.711A** and **G.729** in the **Audio Codec** column of the table.
2. **Media encryption SRTP** and **SRTCP** has been configured, sample values shown in the Media encryption portion.
3. **Encrypted SRTCP** is set to **Best-effort.**
4. **Media encryption** 1-srtp-aescm128-hmac80.
5. **Media encryption** 7-srtp-aescm128-hmac80-unenc-unauth.
6. Default values can be used for all other fields.

Avaya Aura CM: Codec Configuration

```
change ip-codec-set 2                                          Page   1 of   2

                         IP MEDIA PARAMETERS
   Codec Set: 2

   Audio          Silence       Frames    Packet
   Codec          Suppression   Per Pkt   Size(ms)
1: G.711MU            n            2         20
2: G.711A             n            2         20
3: G.729              n            2         20
4:
5:
6:
7:

    Media Encryption                      Encrypted SRTCP: best-effort
1: 1-srtp-aescm128-hmac80
2: 7-srtp-aescm128-hmac80-unenc-unauth
3:
4:
5:

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Signaling Group

Three signaling groups are configured in the tekVizion lab environment.

1. **Signaling-group 4** is used to support communication between SM and CM for SIP phone registration and features.
2. **Signaling-group 6** is used to communicate to the Avaya Communication Manager Messaging.
3. **Signaling-group 10** is used to support PSTN calling on ISDN-PRI.

Use the **add signaling-group n** command to create a signaling group system where **n** is the signaling group number used in this example.

Signaling Group 4

The following are examples used in the Signaling Group.

1. **Group Number: 4**.
2. **Group Type**: **sip**.
3. **Transport Method**: **TLS**.
4. **Peer Server**: **SM**.
5. **Near-end Node Name**: **procr**.
6. **Near-end Listen Port**: **5061**.
7. **Far-end Node Name**: **Lab133-SM80**.
8. **Far-end Listen Port**: **5061**.
9. **Far-end Network Region**: **2**.
10. **Far-end Domain**: **lab.tekvizion.com**.
11. **Direct IP-IP Audio Connections**? **N**; This setting leaves the Media Gateway in the Media flow from and to the Avaya phones and the Crestron Mercury.

Avaya Aura CM: Signaling Group Configuration for phones

```
display signaling-group 4                                        Page   1 of   2
                              SIGNALING GROUP

 Group Number: 4          Group Type: sip
   IMS Enabled? n       Transport Method: tls
         Q-SIP? n
      IP Video? n                                   Enforce SIPS URI for SRTP? n
   Peer Detection Enabled? y  Peer Server: SM                       Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr              Far-end Node Name: Lab133-SM80
 Near-end Listen Port: 5061             Far-end Listen Port: 5061
                                      Far-end Network Region: 2

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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Signaling Group 6

The following are examples used in the Signaling Group.

1. **Group Number**: **6**.
2. **Group Type**: **sip**.
3. **Transport Method**: **TLS**.
4. **Near-end Node Name**: **procr**.
5. **Near-end Listen Port**: **5061**.
6. **Far-end Node Name**: **acmm**.
7. **Far-end Listen Port**: **5061**.
8. **Far-end Network Region**: **1**.
9. **Far-end Domain**: **lab.tekvizion.com**.

Avaya Aura CM: Signaling Group Configuration for PSTN

```
display signaling-group 6                                        Page   1 of   2
                              SIGNALING GROUP

 Group Number: 6            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: Others                   Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr              Far-end Node Name: acmm
 Near-end Listen Port: 5061             Far-end Listen Port: 5061
                                       Far-end Network Region: 1

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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Signaling Group 10

The following are examples used in the Signaling Group.

1. **Group Number**: **10**.
2. **Group Type**: **isdn-pri**.
3. **Primary D-channel**, **001V224**

Avaya Aura CM: Signaling Group Configuration for PSTN

```
display signaling-group 10                                    Page   1 of   5
                              SIGNALING GROUP

 Group Number: 10             Group Type: isdn-pri
                     Associated Signaling? y          Max number of NCA TSC: 0
                       Primary D-Channel: 002V224      Max number of CA TSC: 0
                                                     Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 10       X-Mobility/Wireless Type: NONE
      TSC Supplementary Service Protocol: a          Network Call Transfer? n

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Trunk Groups

Two trunk groups are configured in the tekVizion lab environment.

1. **Trunk Group 4** to access the stations registered to the Avaya Session Manager.
2. **Trunk Group 10** to send 10/11 digit calling number to PRI trunk or PSTN.

Use the add **trunk-group n** command used to add a new trunk group. (Where **n** is the trunk group number).

Trunk Group 4 – To SM

The following are examples used in the Trunk Group.

1. **Group Number**: **4**.
2. **Group Name**: **CNOIP TG**.
3. **Group Type**: **sip**.
4. **Service Type**: **tie**.
5. **TAC**: **#004**.
6. **Signaling Group**: **4**.
7. **Number of Members**: **5**.
8. **Preferred Minimum Session Refresh Interval (Sec): 900.**
9. **Numbering Format: private**

Avaya Aura: Trunk Group to SM (1/4)

```
display trunk-group 4                                          Page   1 of   4
                              TRUNK GROUP

Group Number: 4                Group Type: sip          CDR Reports: y
  Group Name: CNOIP TG                 COR: 1        TN: 1        TAC: #004
   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: 4
                                            Number of Members: 5

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Avaya Aura: Trunk Group to SM (2/4)

```
display trunk-group 4                                          Page   2 of   4
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                          Redirect On OPTIM Failure: 5000

            SCCAN? n                                Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900

 Disconnect Supervision - In? y  Out? y


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




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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Avaya Aura CM: Trunk Group to SM (3/4)

```
display trunk-group 4                                          Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                            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


F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Avaya Aura CM: Trunk Group to SM (4/4)

```
display trunk-group 4                                          Page   4 of   4
                              PROTOCOL VARIATIONS

                                      Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? n

                                    Send Diversion Header? n
                                  Support Request History? n
                             Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? y
                        Identity for Calling Party Display: From
            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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Trunk Group 20 – To ACMM

The following are examples used in the Trunk Group.

1. **Group Type**: **sip**.
2. **Service Type**: **public-ntwrk**.
3. **Signaling Group**: **6**.
4. **Number of Members**: **10**.

Avaya Aura CM: Trunk Group to ACMM (1/4)

```
display trunk-group 20                                         Page   1 of   4
                                TRUNK GROUP

Group Number: 20                 Group Type: sip          CDR Reports: y
  Group Name: OUTSIDE CALL                COR: 1        TN: 1        TAC: #020
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                          Member Assignment Method: auto
                                                   Signaling Group: 6
                                                 Number of Members: 10

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Avaya Aura CM: Trunk Group to ACMM (2/4)

```
display trunk-group 20                                          Page   2 of   4
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                         Redirect On OPTIM Failure: 5000

            SCCAN? n                              Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


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




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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Avaya Aura CM: Trunk Group to ACMM (3/4)

```
display trunk-group 20                                          Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n           Measured: none
                                                      Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                            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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Avaya Aura CM: Trunk Group to ACMM (4/4)

```
display trunk-group 20                                          Page   4 of   4
                              PROTOCOL VARIATIONS

                                      Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                        Send Transferring Party Information? n
                                   Network Call Redirection? n

                                     Send Diversion Header? y
                                   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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Trunk Group 10 – To PSTN

The following are examples used in the Trunk Group.

1. **Group Number**: **10**.
2. **Group Name**: **T1**.
3. **Group Type**: **isdn**.
4. **Service Type**: **public-ntwrk**.
5. **TAC**: **#010**.

Avaya Aura CM: Trunk Group to PRI/PSTN

```
display trunk-group 10                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 10                  Group Type: isdn          CDR Reports: y
  Group Name: T1                          COR: 1        TN: 1        TAC: #010
   Direction: two-way        Outgoing Display? n         Carrier Medium: PRI/BRI
 Dial Access? n              Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Route Pattern

The route pattern defines which trunk group is used for the call and performs any necessary digit manipulation. Use the change **route pattern n** command, where **n** is the route pattern number to configure the parameters for the PSTN trunk route pattern.

- **Route pattern**: **4** is used for calling extensions via Avaya Aura Session manager.

Avaya Aura CM: Route Pattern for SIP phones

```
display route-pattern 4                                          Page   1 of   4
                   Pattern Number: 4      Pattern Name: CNoIP RP
   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: 4    0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

- **Route pattern**: **20** is used for routing calls to the voice mail system, Avaya CMM.

Avaya Aura CM: Route Pattern for Avaya CMM

```
display route-pattern 20                                         Page   1 of   4
                   Pattern Number: 20     Pattern Name: CMM
   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: 20   0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

- **Route pattern**: **10** is used for calling PSTN.

Avaya Aura CM: Route Pattern for PSTN (PRI)

```
display route-pattern 10                                          Page   1 of   4
                    Pattern Number: 10     Pattern Name: T1
   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: 10   0                                                            n   user
 2:                                                                   n   user
 3:                                                                   n   user
 4:                                                                   n   user
 5:                                                                   n   user
 6:                                                                   n   user

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

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Outbound Routing

Auto Alternative Routing (AAR)

The Auto Alternative Routing (AAR) feature is used to route calls to Crestron Mercury & PBX extensions, along with calls to the Voice Mail System – ACMM.

AAR Analysis 66 – Crestron Mercury and PBX Extensions

1. **Dialed String**: **66.**
2. **Total Min and Max**: used **4** for the extensions.
3. **Route Pattern**: **4.**
4. **Call Type**: **unku.**
5. **ANI Regd: N.**

Avaya Aura CM: Auto Alternative Routing analysis 66

```
display aar analysis 66                                           Page   1 of   2
                          AAR DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 3

          Dialed          Total     Route    Call    Node   ANI
          String         Min  Max  Pattern   Type    Num    Reqd
   66                     4    4     4       unku           n
```

AAR Analysis 5000 – Voice Mail System – ACCM

1. **Dialed String**: **5000.**
2. **Total Min and Max**: used **4** to access the Communication Manager Messenger.
3. **Route Pattern**: **20.**
4. **Call Type**: **aar.**
5. **ANI Regd: N.**

Avaya Aura CM: Auto Alternative Routing analysis 5000

```
display aar analysis 5000                                    Page   1 of   2
                          AAR DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 3

         Dialed           Total     Route    Call   Node  ANI
         String          Min  Max  Pattern   Type   Num   Reqd
   5000                  4    4     20       aar          n
```

Automatic Route Selection (ARS)

The Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the PSTN.

1972 – PSTN phone access

1. **Dialed String**: **1972.**
2. **Total Min and Max**: used **11** to allow 10 and 11 digit dialing to PSTN.
3. **Route Pattern**: **10.**
4. **Call Type**: **natl.**
5. **ANI Regd: N.**

Avaya Aura CM: Auto Routing Selection Analysis -1972

```
display ars analysis 1972                                    Page   1 of   2
                          ARS DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 3

         Dialed           Total     Route    Call   Node  ANI
         String          Min  Max  Pattern   Type   Num   Reqd
   1972                  11   11    10       natl         n
```

1800 – Toll-Free access

1. **Dialed String**: **1800.**
2. **Total Min and Max**: used **11** to allow 10 and 11 digit dialing to PSTN.
3. **Route Pattern**: **10.**
4. **Call Type**: **natl.**
5. **ANI Regd: N.**

Avaya Aura CM: Auto Routing Selection Analysis -1800

```
display ars analysis 1800                                    Page   1 of   2
                          ARS DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 3

        Dialed          Total     Route    Call    Node  ANI
        String         Min  Max  Pattern   Type    Num   Reqd
  1800                  11   11    10       natl          n
```

Inbound Routing

Inc-Call-Handling-Trmt Trunk-Group

DID numbers received from PSTN are mapped to extensions using the incoming call handling treatment of the receiving trunk group. Use the change **inc-call-handling-trmt trunk-group** command to create an entry for each DID number.

PSTN to Avaya Aura CM – Trunk-Group 10

1. In the tekVizion lab environment, DIDs starting with 972xxx264x are used.
2. The **inc-call-handling-trmt** on the **trunk-group 10** (used to route the inbound calls from PSTN) is configured to delete the first 10 digits and insert the 4-digit extensions.

Avaya Aura CM: Inc-Call-Handling-Trmt Trunk-Group 10

```
display inc-call-handling-trmt trunk-group 10                Page   1 of   3
                    INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert            Per Call Night
 Feature        Len      Digits                           CPN/BN   Serv
 public-ntwrk    10 972[redacted]2640       10  6631
 public-ntwrk    10 972[redacted]2641       10  6632
 public-ntwrk    10 972[redacted]2644       10  6637
 public-ntwrk    10 972[redacted]2645       10  6638
```

Avaya Aura CM to Avaya Aura SM – Trunk-Group

- The **inc-call-handling-trmt** on the **trunk-group 4** (used to route the 10-digit internal calls for extension to extension calling) is configured to delete the first 10 digits and insert the 4-digit extensions.

Avaya Aura CM: Inc-Call-Handling-Trmt Trunk-Group 4

```
display inc-call-handling-trmt trunk-group 4                    Page   1 of   3
                      INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 tie             10                  6   2651
 tie             10                  6   2654
 tie             10                      9
 tie             10                      9
 tie             10                      9
 tie             10 972[redacted]2640   10   6631
 tie             10 972[redacted]2641   10   6632
 tie             10 972[redacted]2643   10   6633
 tie             10 972[redacted]2644   10   6637
 tie             10 972[redacted]2645   10   6638
```

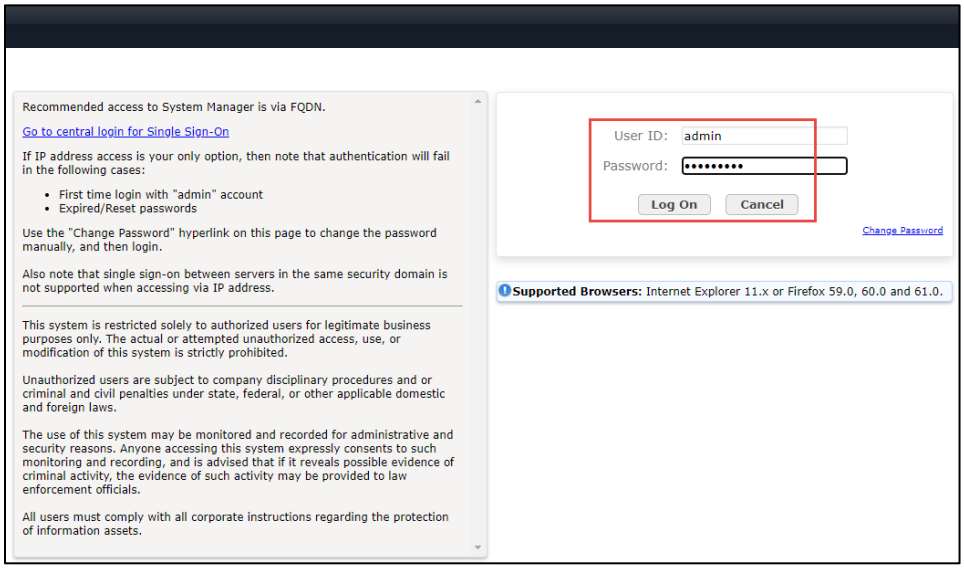
Avaya Aura Session Manager Configuration

Avaya Aura System Manager

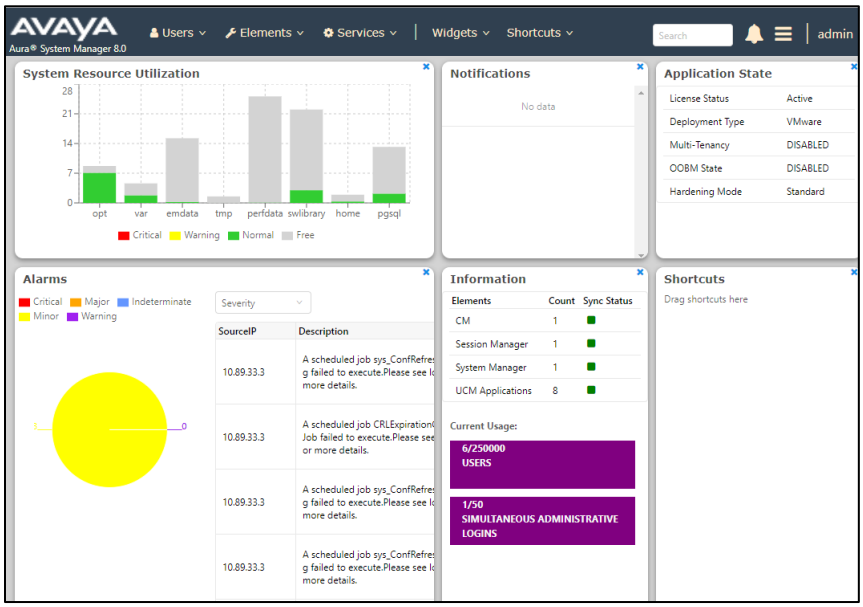
The Avaya Aura Session Manager configuration is performed from the Avaya Aura System Manager

1. Access Avaya Aura System Manager Web login screen via https://<IP Address/FQDN>. IP address *10.89.33.3* is used in this example.
2. Log in with the User Id as admin and associated password, and then click **Log On**.

Avaya Aura System Manager: Login Screen



Avaya Aura System Manager: Navigation Menu



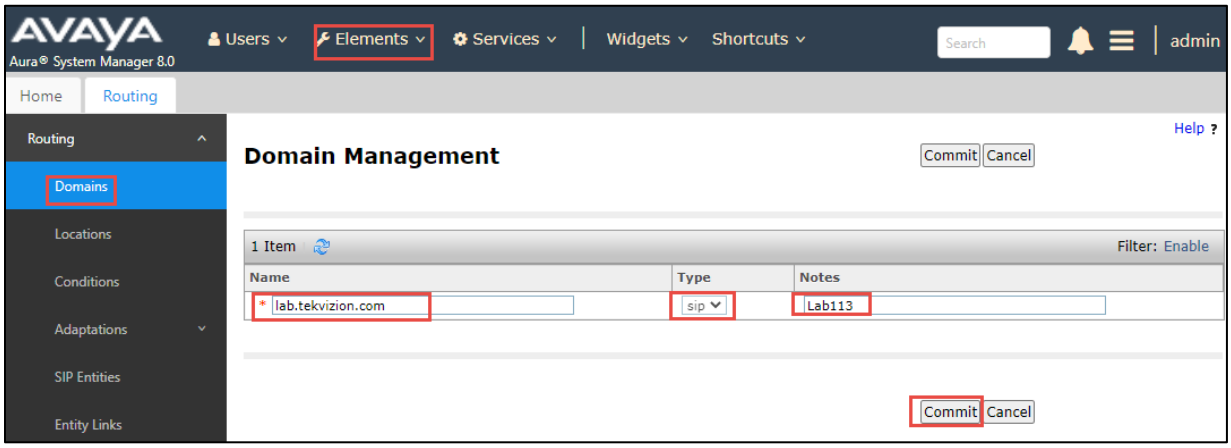
Session Manager - Domain

Create a SIP Domain for each domain that the Session Manager needs to be aware of, to route calls.

To configure a domain, navigate to: **Elements -> Routing -> Domains**.

1. Click **New.**
2. **Name**: Enter the domain name: **lab.tekvizion.com**.
3. **Type**: Select **sip** from the pull-down menu.
4. **Notes**: Add a brief description (optional).
5. Click **Commit** to save.

Avaya Aura Session Manager: Domain



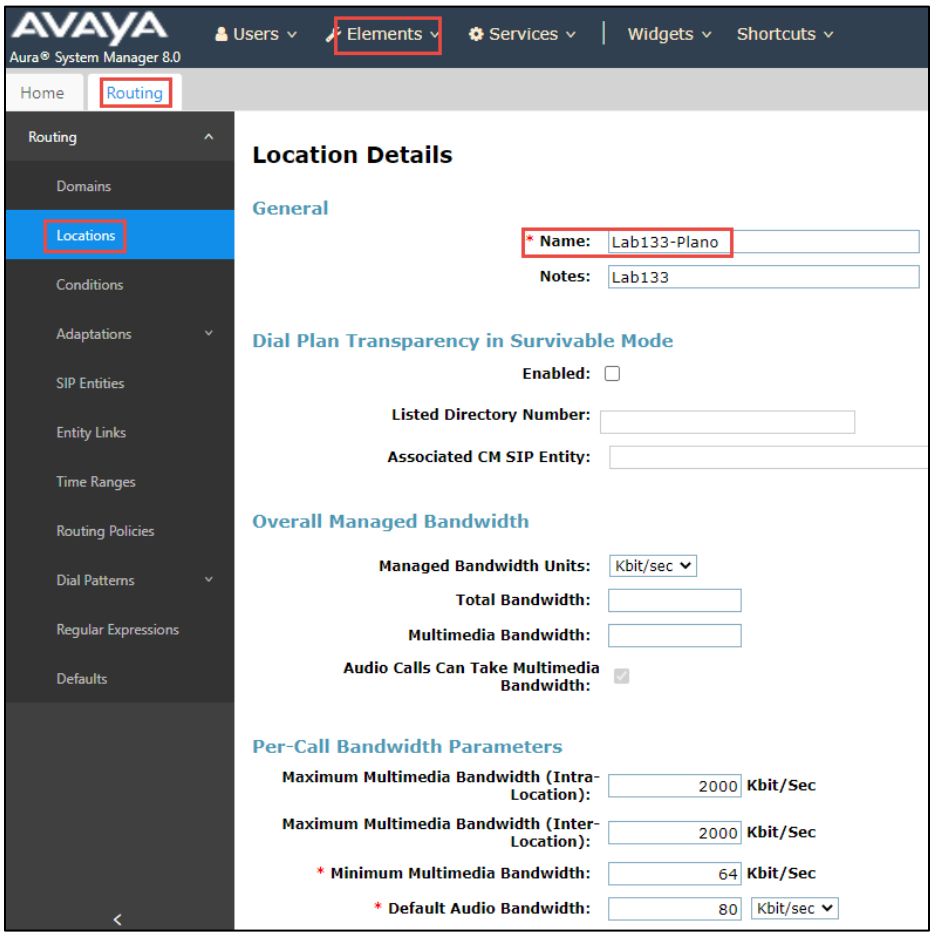
Session Manager - Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management and call admission control.

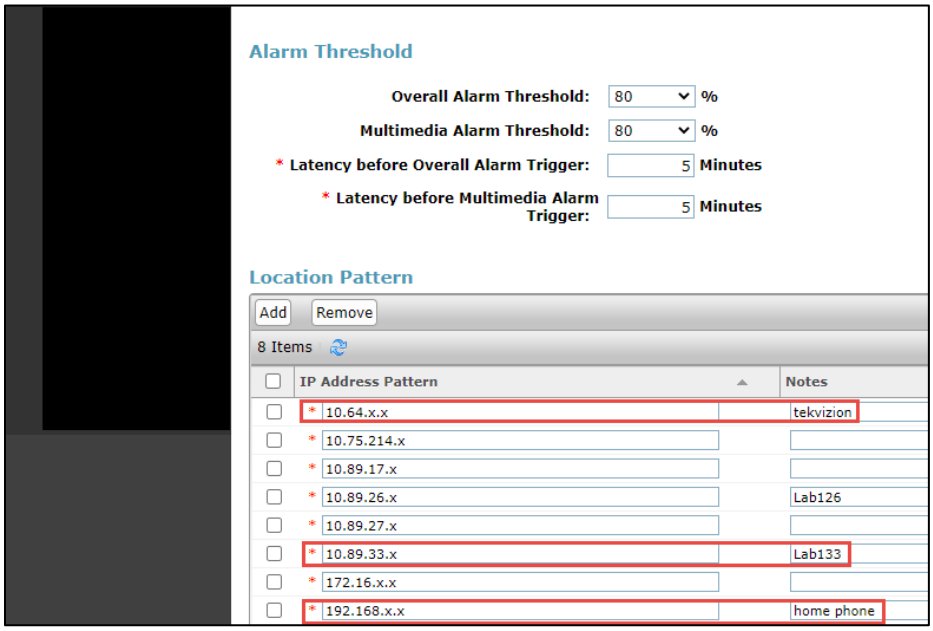
Add a location Navigate to **Routing -> Locations**.

1. **Name**: Enter a descriptive name for the location: **Plano** is used in this example.
2. Provide **Location Patterns** - add IP Address Patterns for different networks that are part of the topology:
   - 10.64.x.x: tekVizion.
   - 10.89.33.x: Avaya Aura 8.0 PBX.
   - 192.186.x.x: Testing lab network.
3. Retain all other default configurations.

Avaya Aura Session Manager: Location



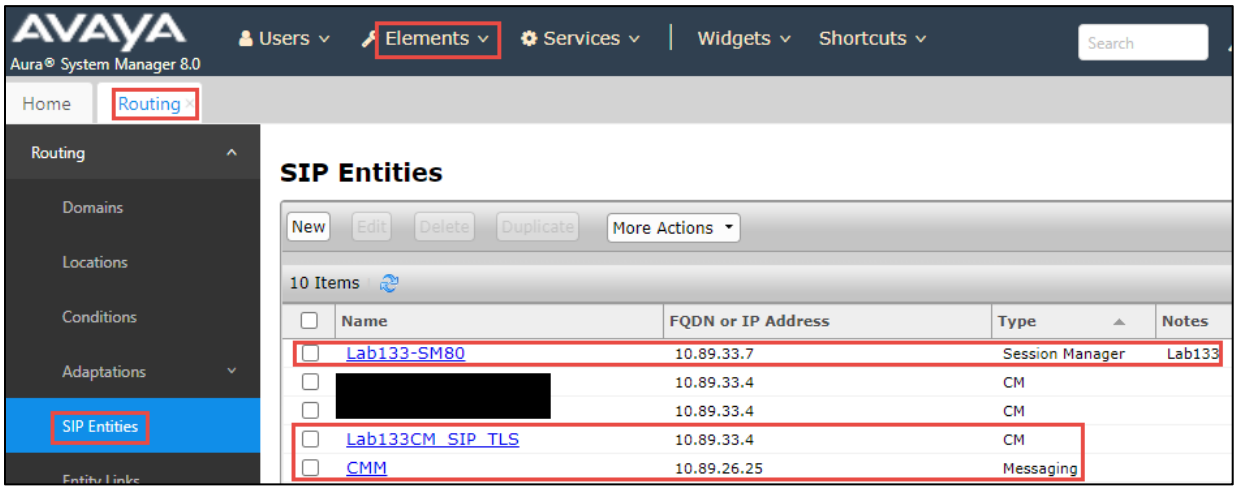
Avaya Aura Session Manager: Location (continued)



SIP Entity

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager, Avaya Communication Manager Messaging Component and the PSTN Gateway.

Avaya Aura Session Manager: SIP Entity

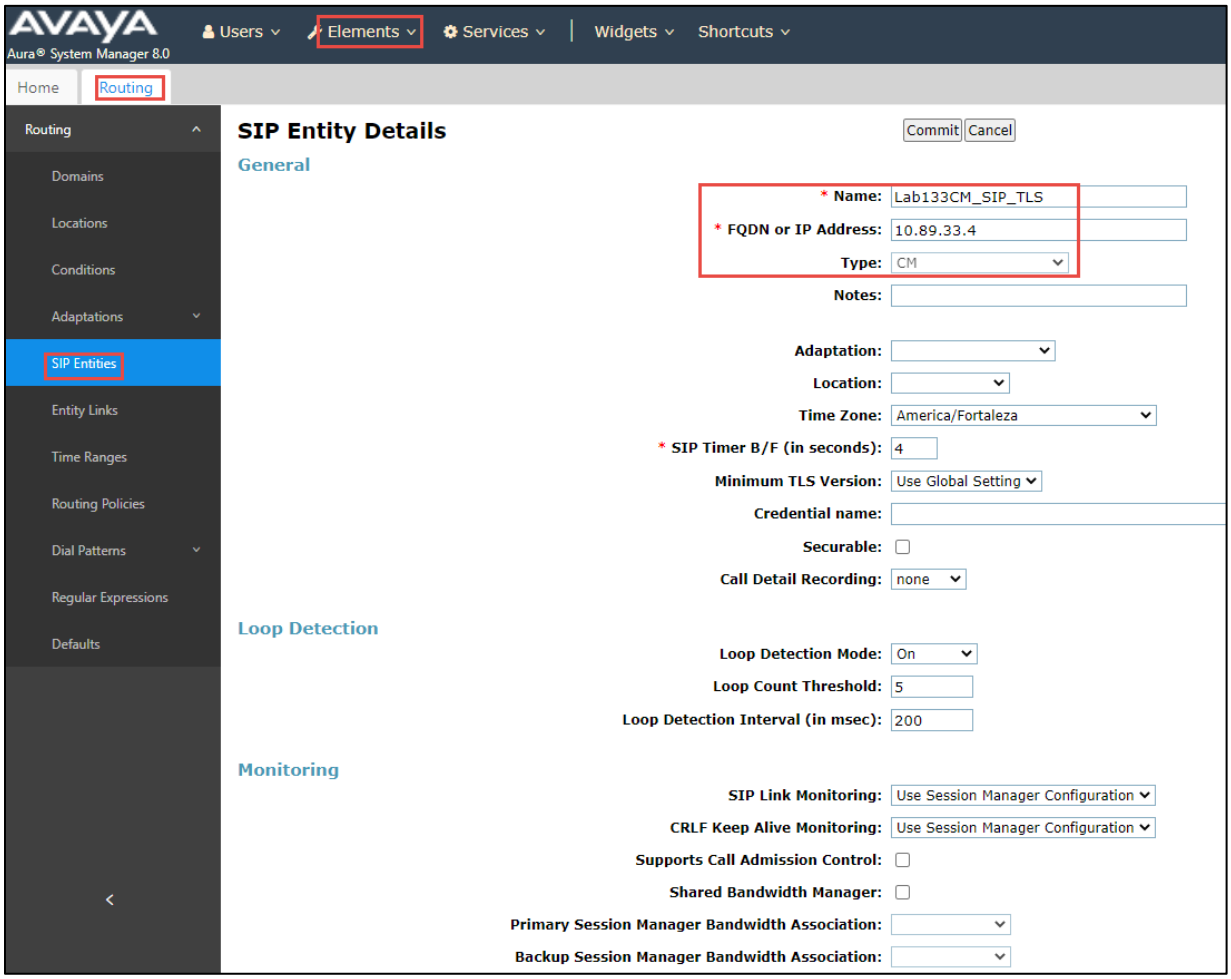


Lab133CM_SIP_TLS

SIP Entity for the Avaya Aura Communication Manager. Navigate to **Routing → SIP Entities.** The following are examples used for the SIP Entity.

1. **Name**: Enter a descriptive name: **Lab133CM_SIP_TLS** used for the Avaya CM.
2. **FQDN or IP Address**: Enter the IP address of the SIP Entity interface that is used for SIP signaling: **10.89.33.4**.
3. **Type**: Enter **CM** for Communication Manager.

Avaya Aura Session Manager: SIP Entity: CM

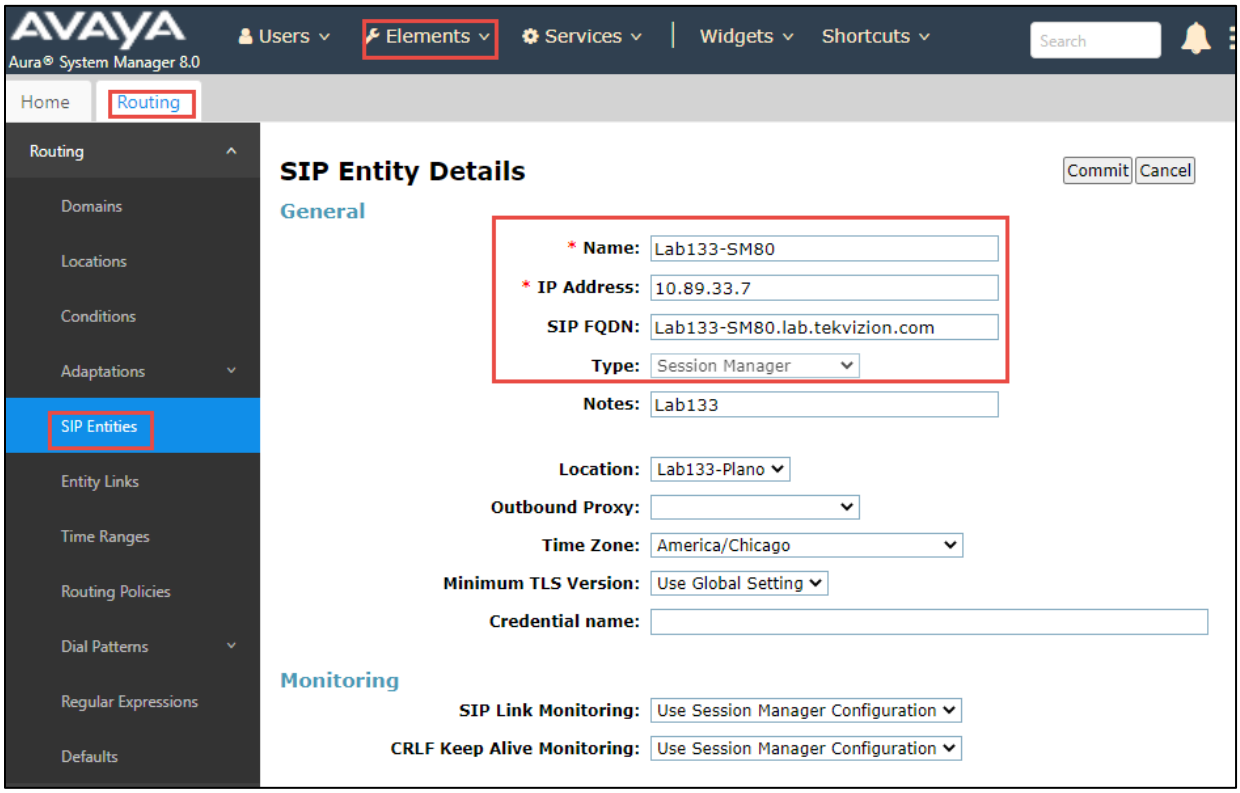


Lab133-SM80

SIP Entity for the Avaya Aura Session Manager. Navigate to **Routing → SIP Entities**. The following are examples used for the SIP Entity.

1. **Name**: Enter a descriptive name: **Lab133-SM80** is used for the Avaya SM.
2. **FQDN or IP Address**: Enter the IP address of the SIP Entity interface that is used for SIP signaling: **10.89.33.7**.
3. **Type**: Enter **SM** for Session Manager.

Avaya Aura Session Manager: SIP Entity: SM

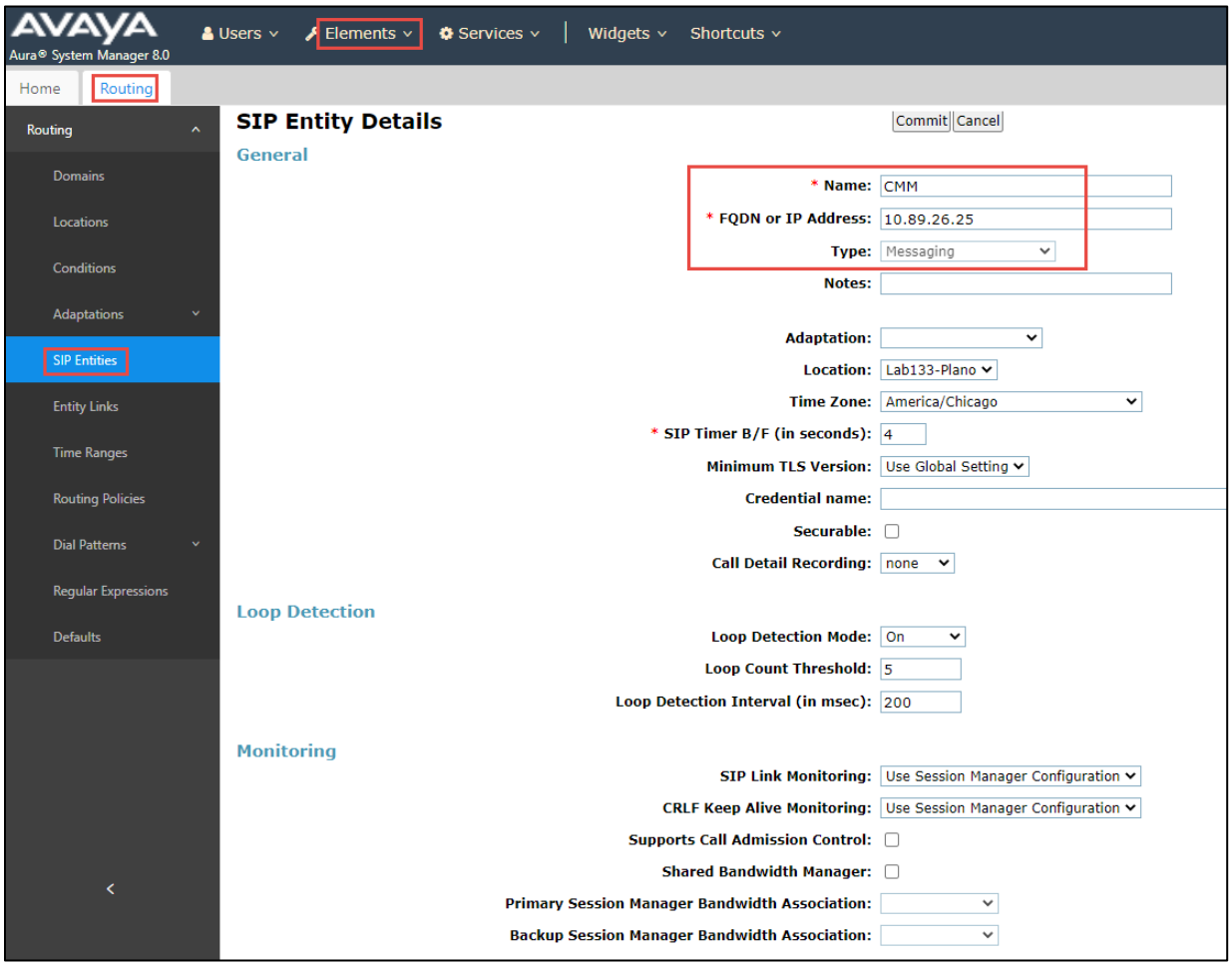


CMM

SIP Entity for the Avaya Aura Communication Manager Messenger. Navigate to **Routing → SIP Entities**. The following are examples used for the SIP Entity.

1. **Name**: Enter a descriptive name: **CMM** is used for the Avaya Communications Manager Messenger.
2. **FQDN or IP Address**: Enter the IP address of the SIP Entity interface that is used for SIP signaling: **10.89.26.25**.
3. **Type**: Enter Messaging for the **CMM**.

Avaya Aura Session Manager: SIP Entity: CMM

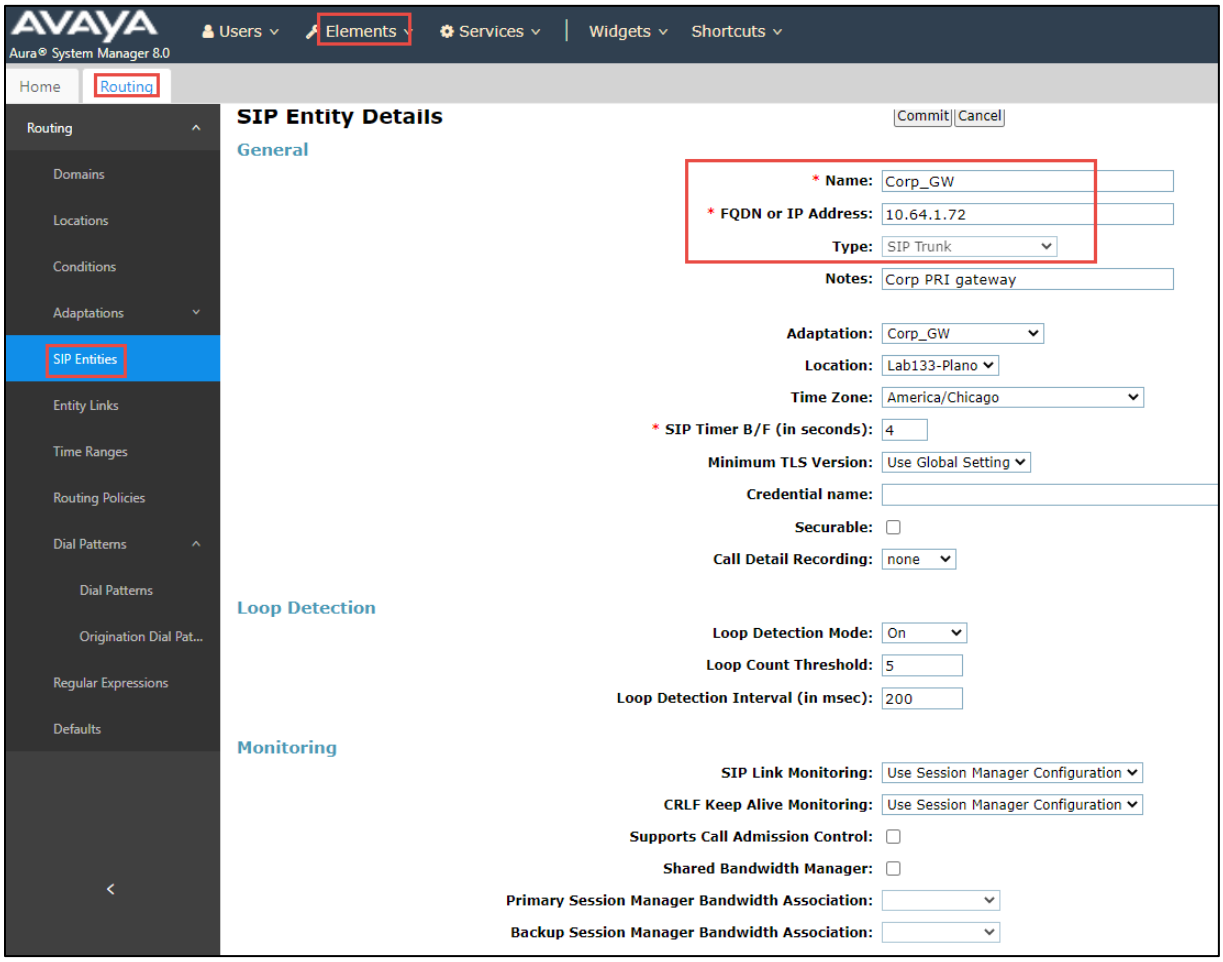


Corp_GW

If using a SIP Trunk to the PSTN Gateway, navigate to **Routing → SIP Entities**. The following are examples used for the SIP Entity.

1. **Name**: Enter a descriptive name: **Corp_GW** is used for the PSTN Gateway.
2. **FQDN or IP Address**: Enter the IP address of the SIP Entity interface that is used for SIP signaling: **10.64.1.72**.
3. **Type**: Enter **SIP Trunk**.

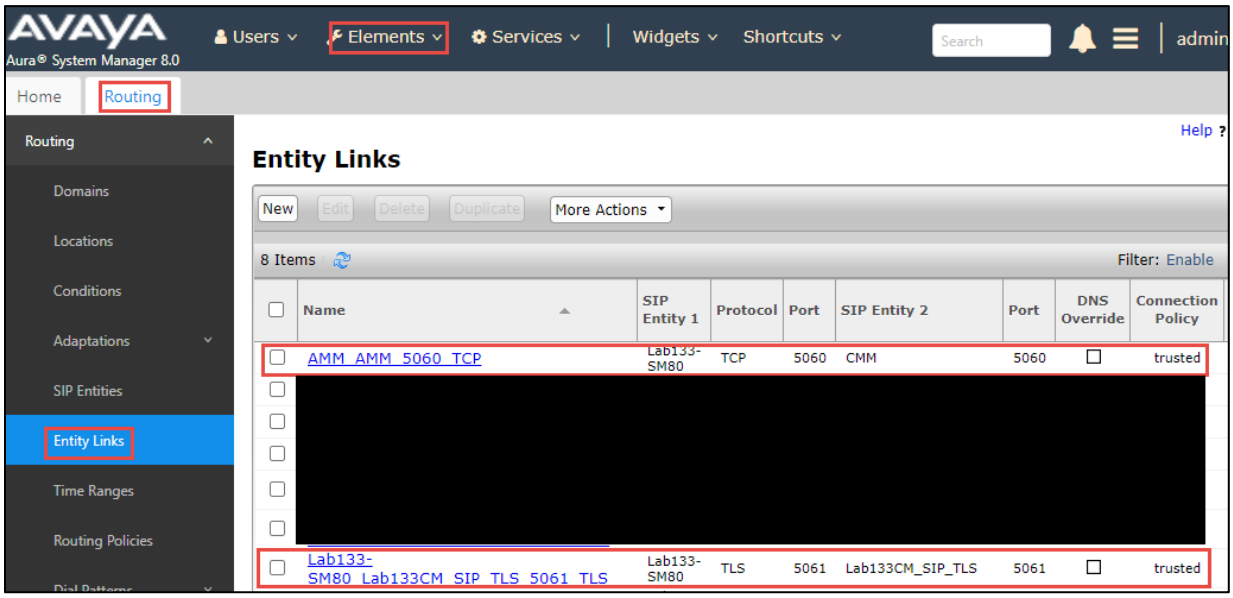
Avaya Aura Session Manager: SIP Entity: PSTN



Entity Links

A SIP trunk between Avaya Aura Session Manager and a telephony system is described by an Entity Link. Entity links are created to the Avaya Aura Communication Manager and the Avaya Aura Communication Manager Messenger.

Avaya Aura Session Manager: Entity Links: CM

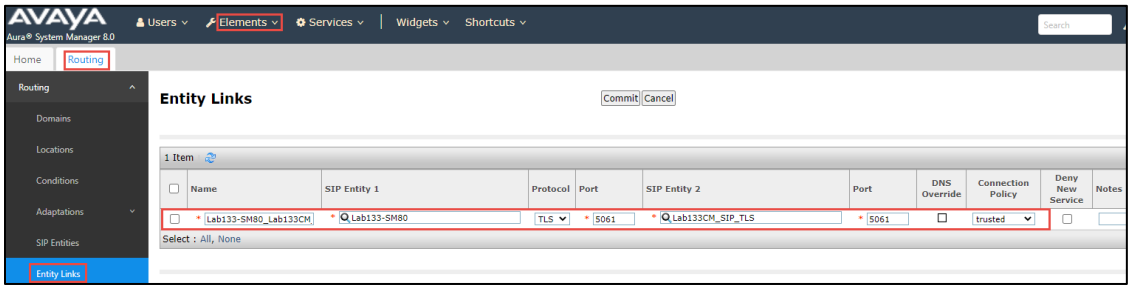


Lab133-SM80_Lab133CM_SIP_TLS_5061_TLS

Avaya Communication Manager Entity Link. Navigate to **Routing → Entity Links.** The following are examples used for the Entity Link.

1. **Name**: Enter a descriptive name, **Lab133-SM80_Lab133CM.**
2. **SIP Entity 1**: select the Session Manager, **Lab133-SM80.**
3. **Protocol**: **TLS**.
4. **Port**: **5061**.
5. **SIP Entity 2**: select the Communication Manager, **Lab133CM_SIP_TLS.**
6. **Port**: **5061**.
7. **Connection Policy**: select **Trusted.**

Avaya Aura Session Manager: Entity Links: CM

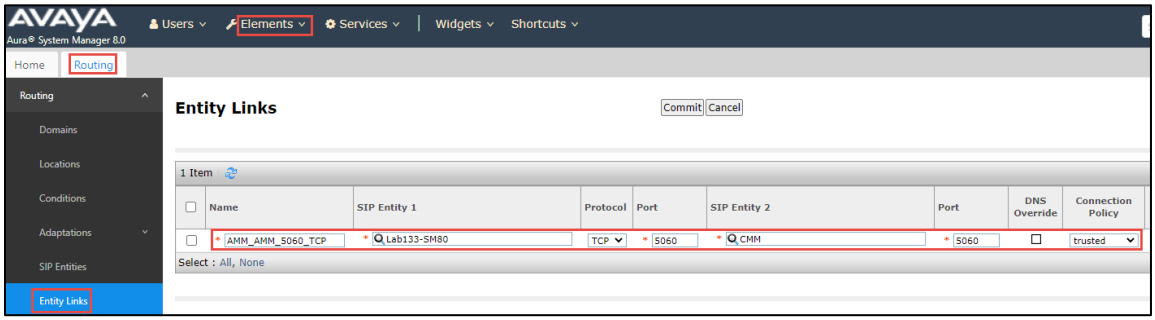


AMM_AMM_5060_TCP

Avaya Communication Manager Messenger – Voice Mail System - Entity Link. The tekVizion lab CMM does not support SRTCP, so a Non-Secure Entity Link is setup between the SM and the CMM. Navigate to **Routing → Entity Links**. The following are examples used for the Entity Link.

1. **Name**: Enter a descriptive name, **AMM_AMM_506_TCP.**
2. **SIP Entity 1**: select the Session Manager, **Lab133-SM80.**
3. **Protocol**: **TCP**.
4. **Port**: **5060**.
5. **SIP Entity 2**: select the Communication Manager Messenger, **CMM.**
6. **Port**: **5060**.
7. **Connection Policy**: select **Trusted.**

Avaya Aura Session Manager: Entity Links: CMM



Users – Crestron Mercury & PBX phones

A user is configured for each Avaya PBX phone and Crestron Mercury phone used in the tekVizion lab environment. Navigate to **Users → User Management → Manage Users.**

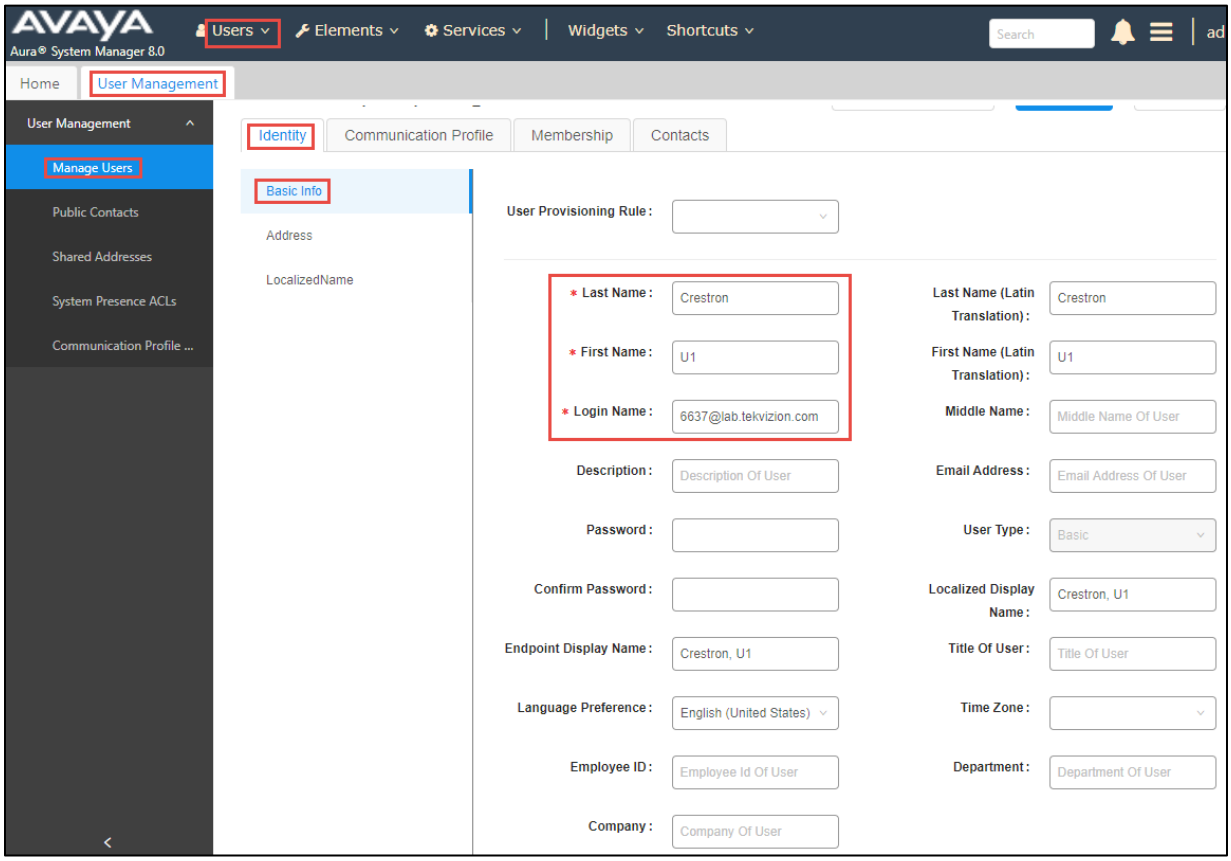
Crestron Mercury phone – Ext 6637

The following are examples used for the User configuration.

Basic Info

1. Click the **Identity** Tab.
2. Select **Basic Info.**
3. Configure **Last Name** and **First Name**: **Crestron U1**.
4. Configure **Login Name**:**6637@lab.tekvizion.com**.

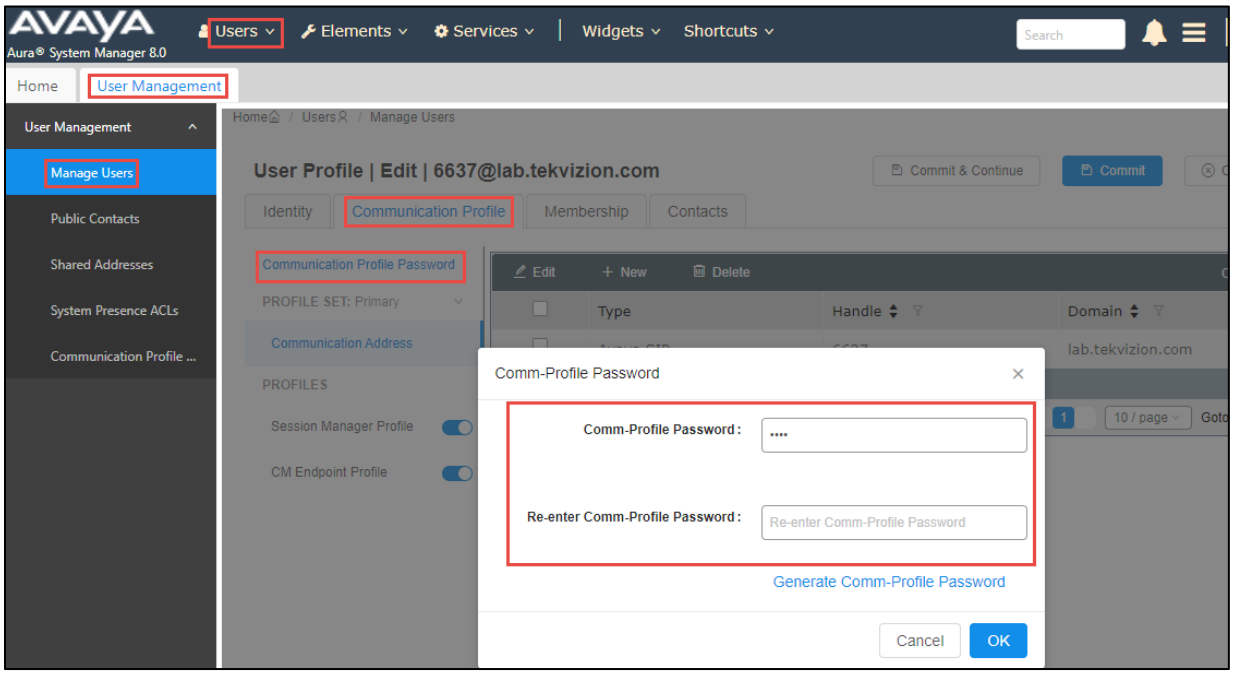
Avaya Aura Session Manager: Crestron Mercury User: Basic Info



Communication Profile - Password

1. Select **Communication Profile** tab.
2. Select **Communication Profile Password**: enter the desired password for the SIP user to use for registration.
3. Confirm Password.

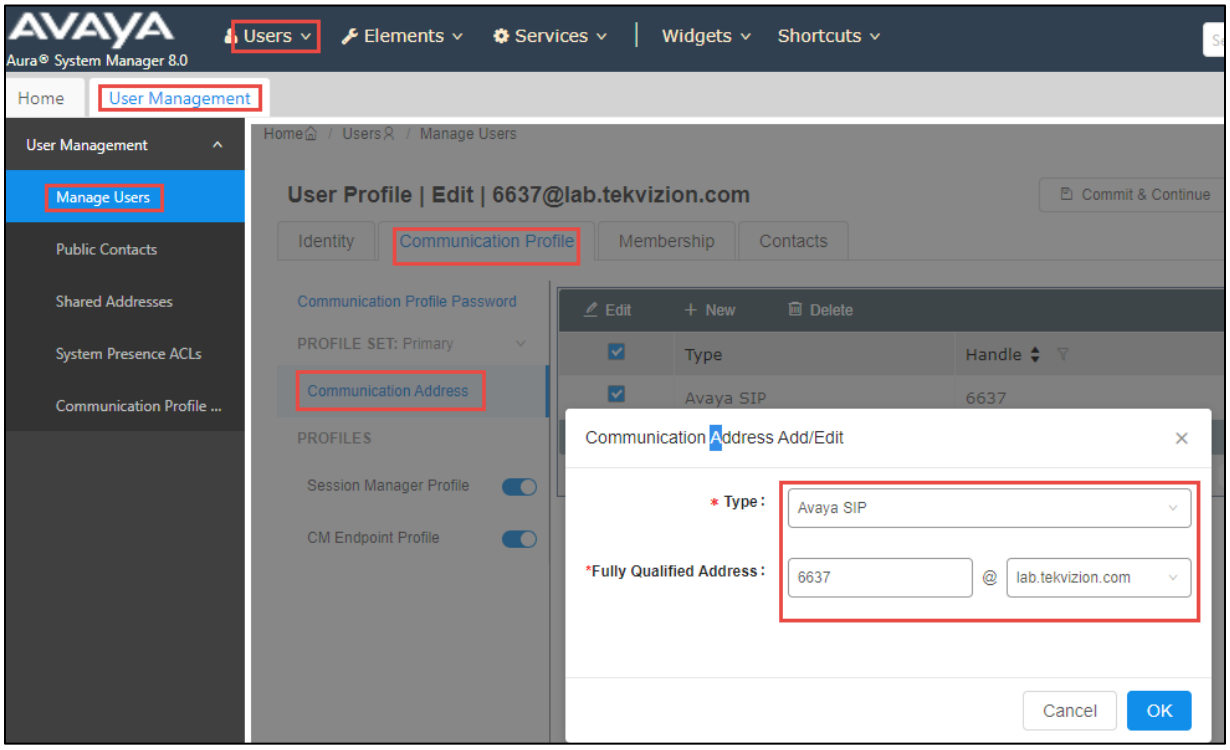
Avaya Aura Session Manager: Crestron Mercury User: Communication Profile: Password



Communication Address

1. Select **Communication Address** link.
2. Select **New.**
3. Select **Avaya SIP**: In the **Type** dropdown box.
4. In the **Fully Qualified Address** add the extension @ Domain example: **6637@lab.tekvizion.com.**

Avaya Aura Session Manager: Crestron Mercury User: Communication Profile: Communication Address

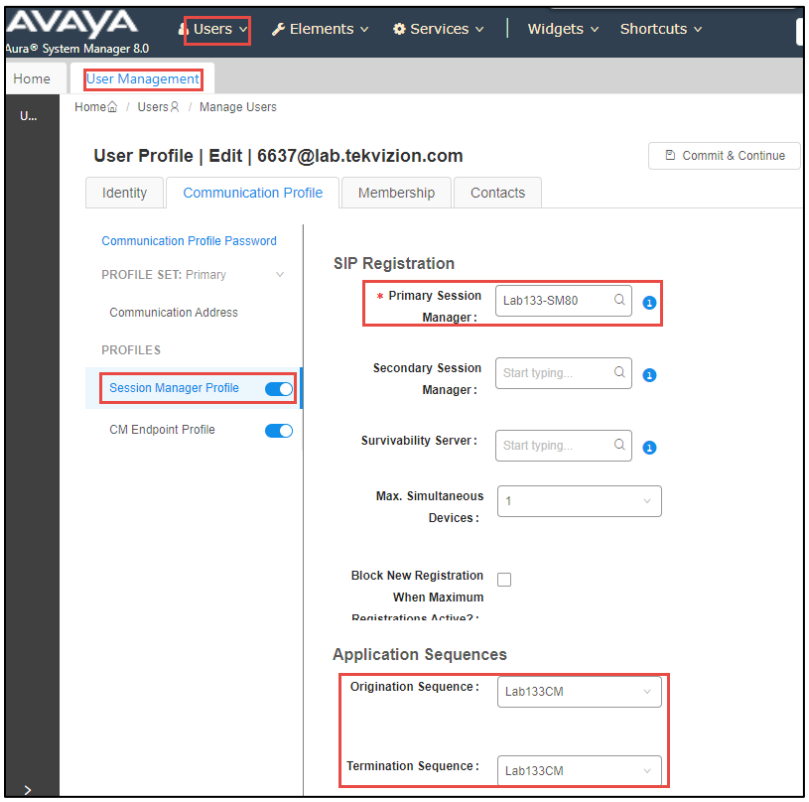


Session Manager Profile

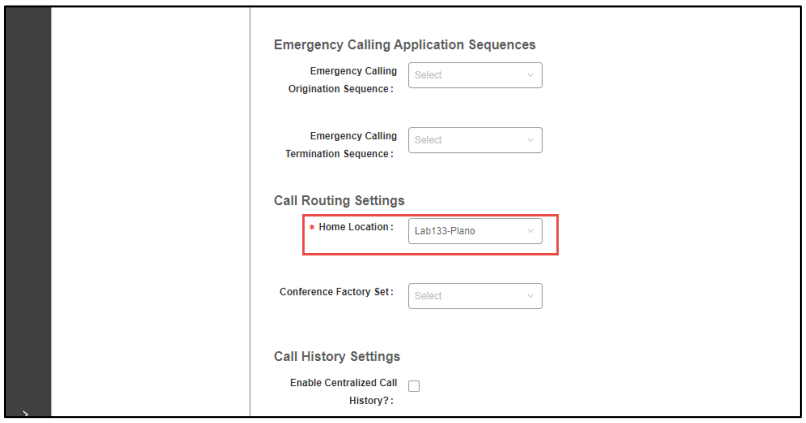
From the **Communication Profile** tab select the **Session Manager Profile.**

1. When Session Manager Profile is selected, the button slides to the right and turns blue.
2. Under **SIP Registration** section for the **Primary Session Manager** select the **SM**, **Lab133-SM80.**
3. Under **Application Sequences** for **Origination Sequence** select the **CM, Lab133CM.**
4. Under **Application Sequences** for **Termination Sequence** select the **CM, Lab133CM.**
5. Under **Call Routing Settings** select the **Home location** of the PBX, **Lab133Plano.**

Avaya Aura Session Manager: Crestron Mercury User: Communication Profile: Session Manager Profile



Avaya Aura Session Manager: Crestron Mercury User: Session Manager Profile (Continued)

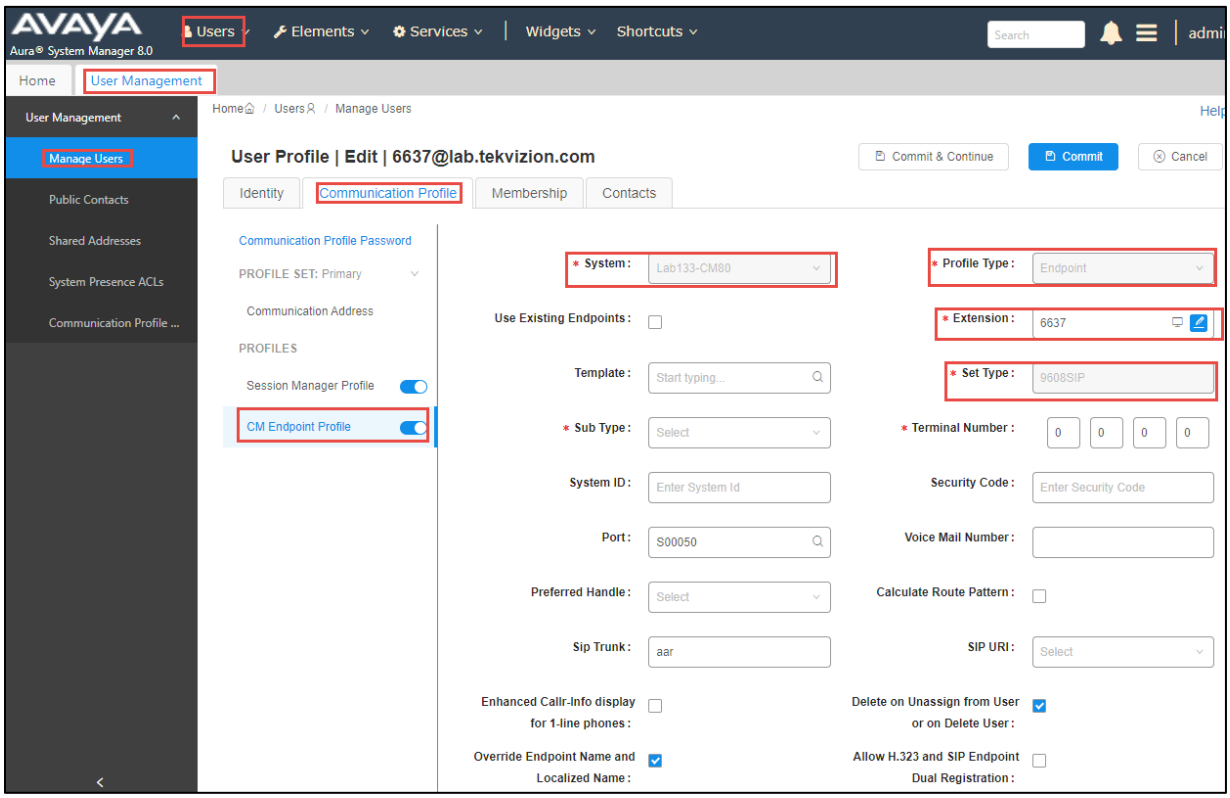


CM Endpoint Profile

From the **Communication Profile** tab select the **CM Endpoint Profile.**

1. When CM Endpoint Profile is selected, the button slides to the right and turns blue.
2. Select the **CM** for the **System** dropdown, **Lab133-CM80.**
3. Select **Endpoint** in the **Profile Type** dropdown.
4. Select the User extension for the **Extension** box, used **6637**.
5. Select the User phone type for the **Set Type** box, used **9608SIP** for the Crestron Mercury phone.

Avaya Aura Session Manager: Crestron Mercury User: Communication Profile: CM Endpoint Profile



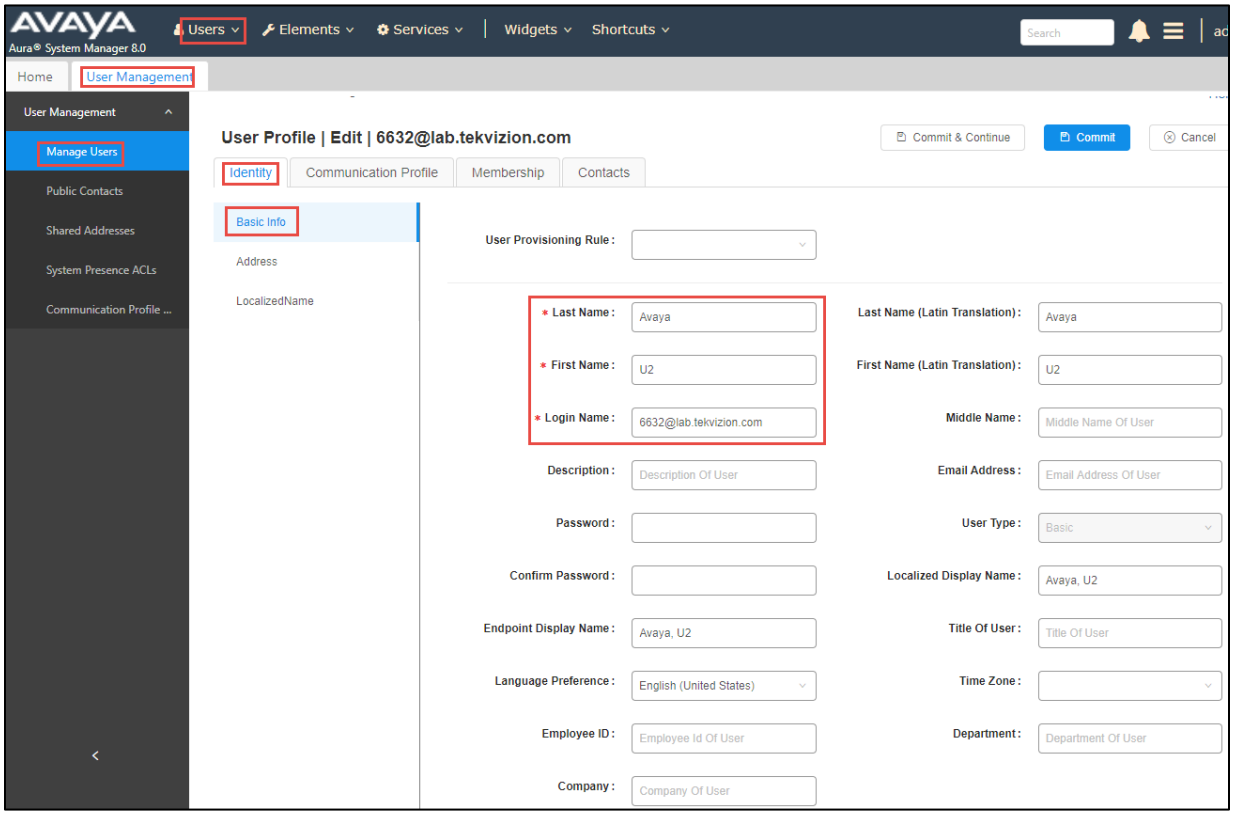
Avaya PBX phone – Ext 6632

The following are examples used for the User configuration.

Basic Info

1. Click the **Identity** Tab and select **Basic Info**.
2. Configure **Last Name** and **First Name**: **Avaya U2**.
3. Configure **Login Name**:**6632@lab.tekvizion.com**.

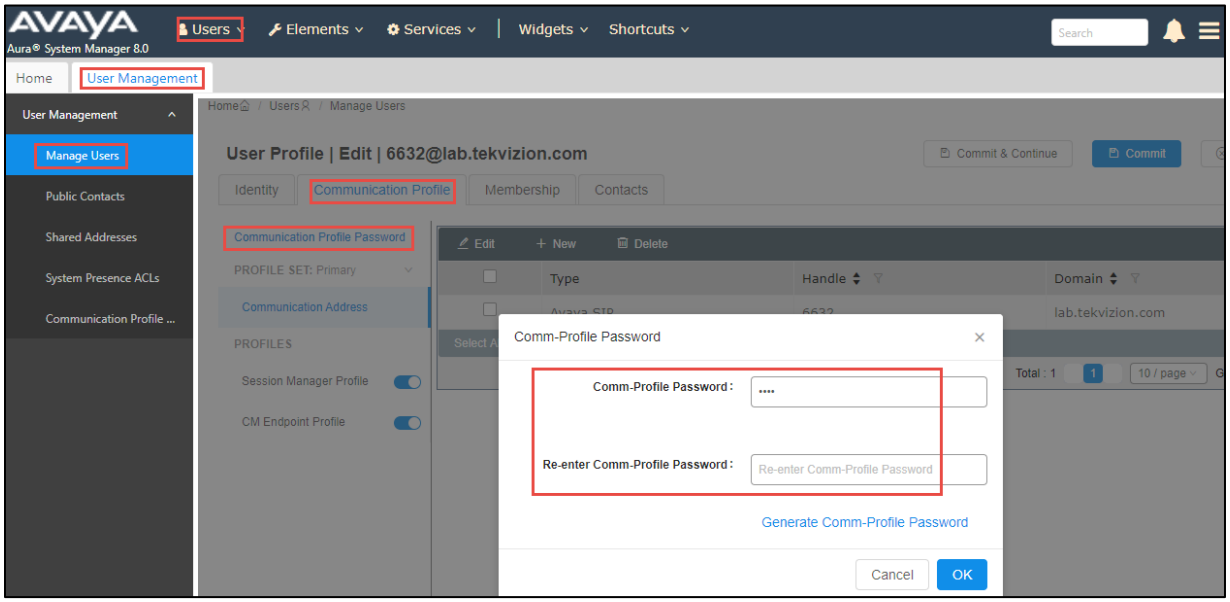
Avaya Aura Session Manager: Crestron Mercury User: Basic Info



Communication Profile - Password

1. Select the **Communication Profile** tab.
2. Select **Communication Profile Password**: enter the desired password for the SIP user to use for registration.
3. Confirm Password.

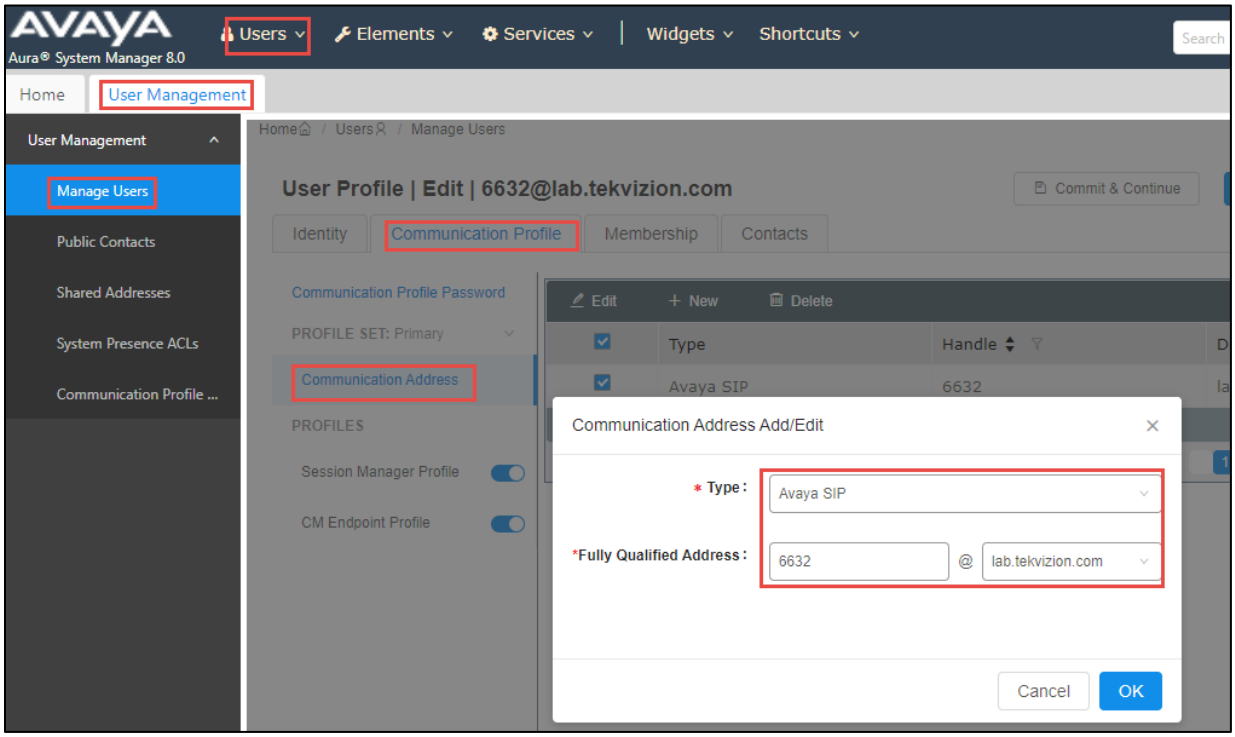
Avaya Aura Session Manager: Crestron Mercury User: Communication Profile: Password



Communication Address

1. Select the **Communication Address** link.
2. Select **New.**
3. Select **Avaya SIP** in the **Type** dropdown box.
4. In the **Fully Qualified Address,** add the extension @ Domain example: **6632@lab.tekvizion.com.**

Avaya Aura Session Manager: Crestron Mercury User: Communication Profile: Communication Address

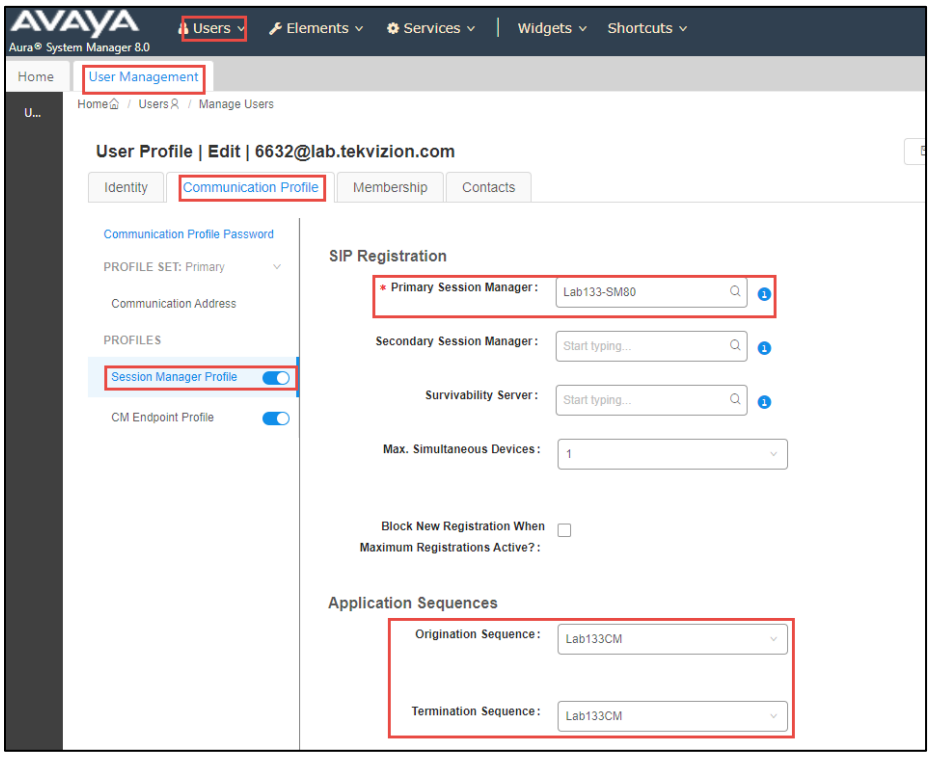


Session Manager Profile

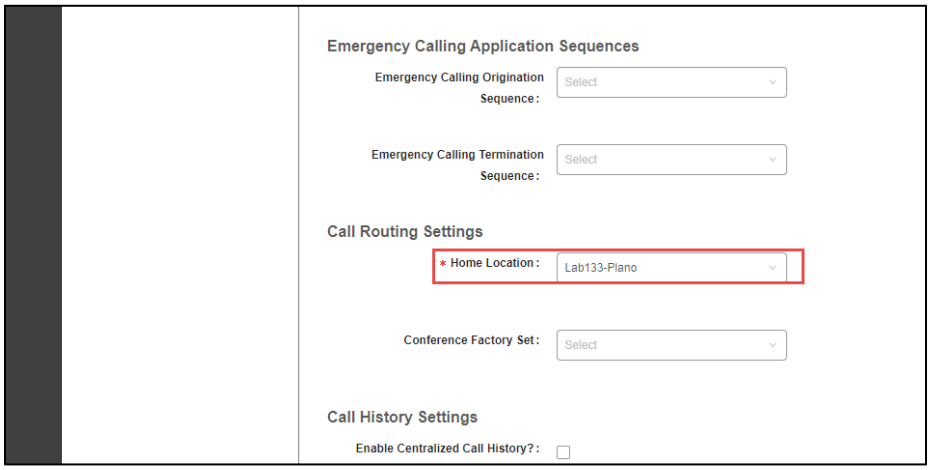
From the **Communication Profile** tab, select the **Session Manager Profile.**

1. The button to the right of the link slides to the right and turns blue.
2. Under **SIP Registration** section for the **Primary Session Manager** select the **SM.**
3. Under **Application Sequences** for **Origination Sequence** select the **CM.**
4. Under **Application Sequences** for **Termination Sequence** select the **CM.**
5. Under **Call Routing Settings** for **Home Location** select the Home location of the PBX.

Avaya Aura Session Manager: Crestron Mercury User: Communication Profile: Session Manager Profile



Avaya Aura Session Manager: Crestron Mercury User: Session Manager Profile (Continued)

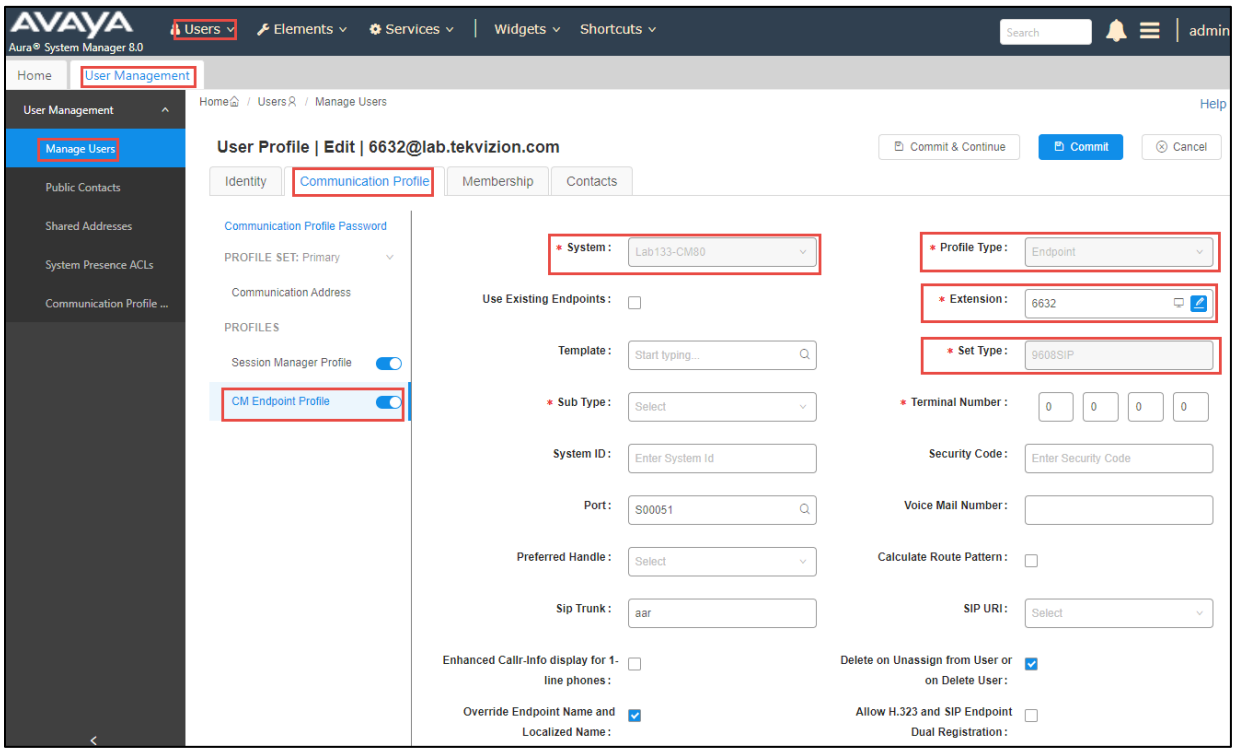


CM Endpoint Profile

From the **Communication Profile** tab select the **CM Endpoint Profile.**

1. The button to the right of the link slides to the right and turns blue.
2. Select the **CM** for the **System** dropdown.
3. Select **Endpoint** in the **Profile Type** dropdown.
4. Select the User extension for the **Extension** box, used **6632**.
5. Select the User phone type for the **Set Type** box, used **9608SIP** for the Avaya PBX phone.

Avaya Aura Session Manager: Crestron Mercury User: Communication Profile: CM Endpoint Profile



Routing Policy

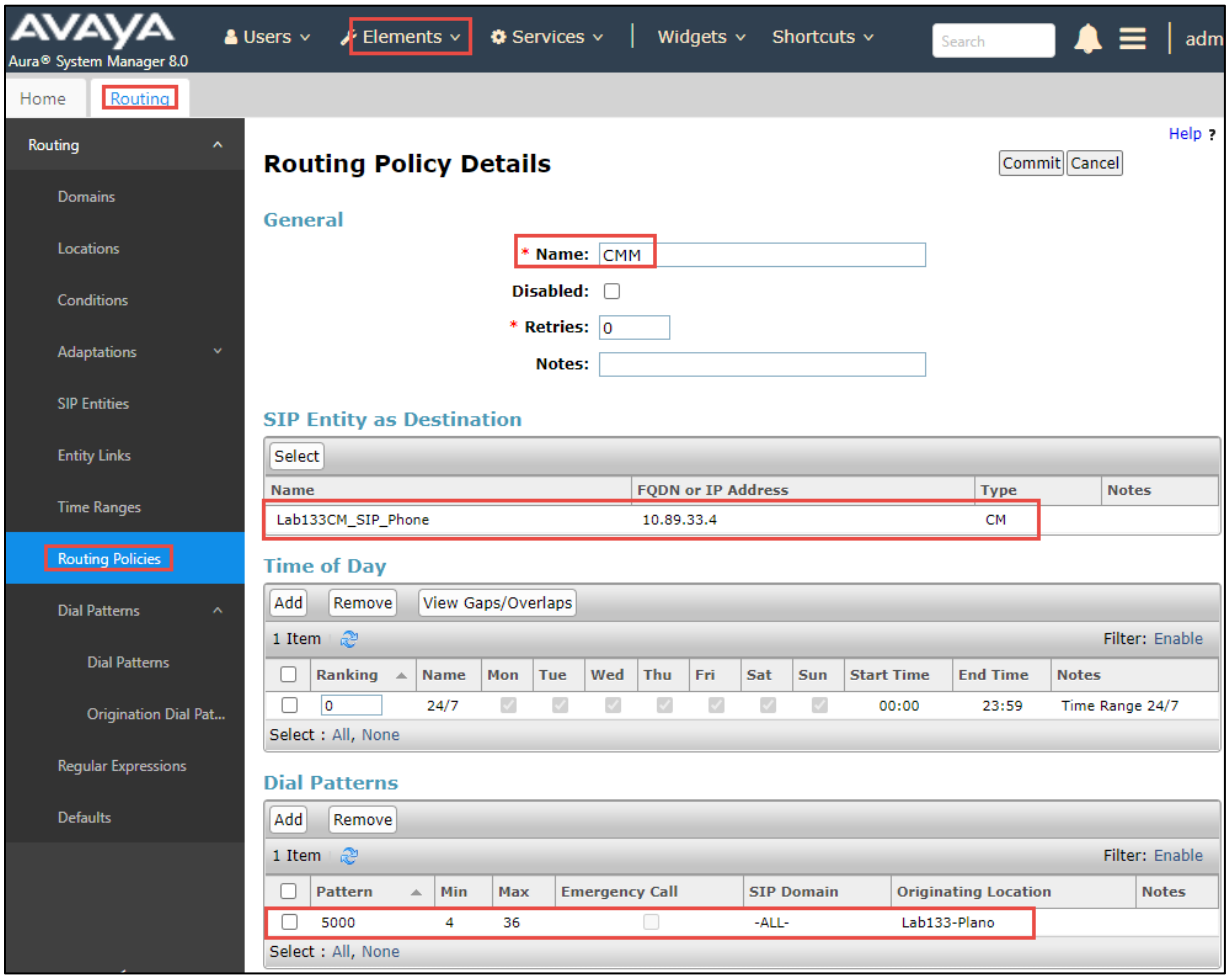
Routing Policies describe the conditions under which calls are routed to the SIP entities. Two routing policies are added: one for voice mail (CMM), and one to the PSTN Gateway.

Routing Policy to Communication Manager Messenger

To add a routing policy for Avaya Communication Manager Messenger. Navigate to **Elements -> Routing -> Routing Policies**. The following are examples used for the Routing Policy.

1. Click **New**.
2. In the General section, enter the following values:
   - **Name**: **CMM**.
   - **SIP Entity as Destination**: Select the SIP Entity **Lab133CM_SIP_Phone**.
   - Retain all other default configurations.
3. Add the **Dial Pattern 5000** to route to the CMM using this policy.

Avaya Aura Session Manager: Routing Policies: CMM

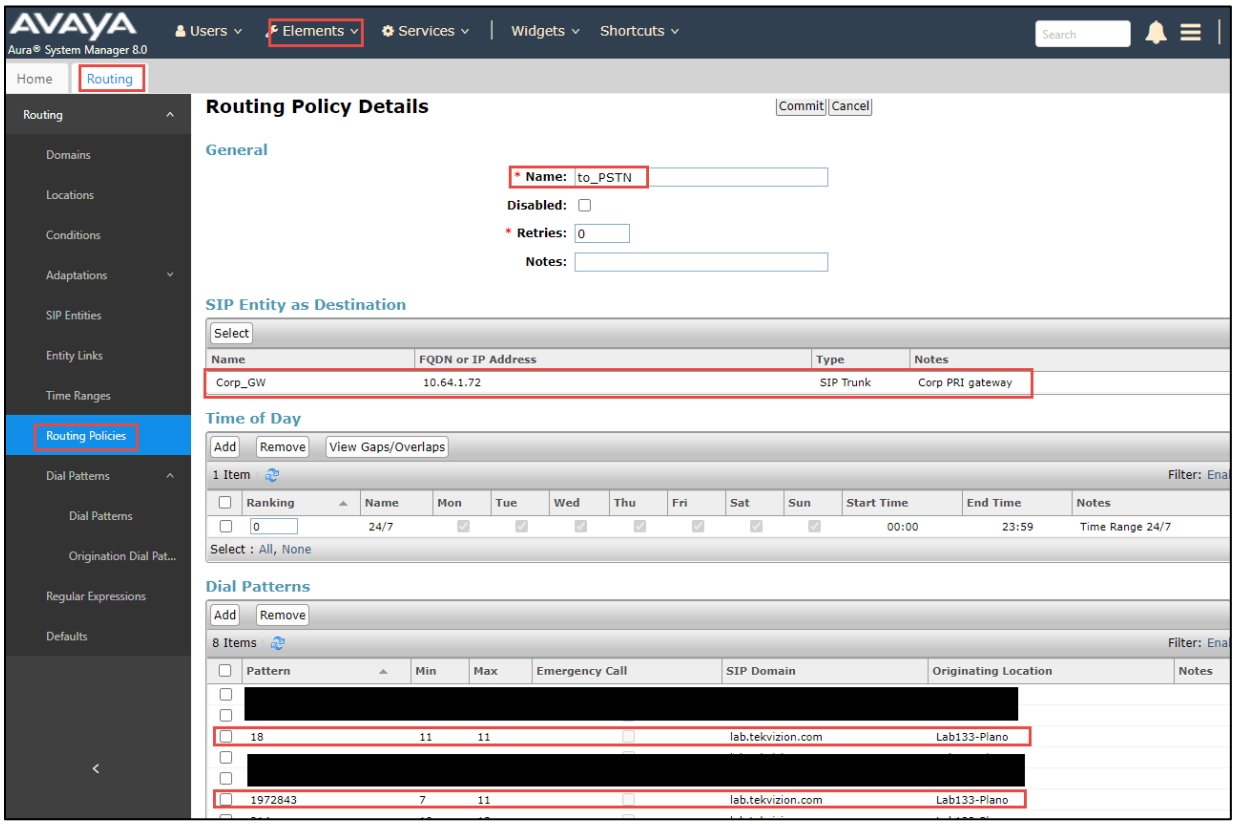


Routing Policy to PSTN Gateway

If using a SIP Trunk to the PSTN Gateway, add a routing policy for the PSTN Gateway. Navigate to **Elements -> Routing -> Routing Policies**. The following are examples used for the Routing Policy.

1. Click **New.**
2. In the **General** section, enter the following values:
   - **Name**: **to_PSTN**.
   - **SIP Entity as Destination**: Select the SIP Entity **Corp_GW**.
   - Retain all other default configurations.
3. Add the following dial patterns that can be routed using this policy:
   - For PSTN calling: the **1972843** Dial pattern is selected.
   - For Toll Free calling: the **18** Dial pattern is selected.

Avaya Aura Session Manager: Routing Policies: PSTN



Dial Patterns

Dial Patterns are created to route outbound calls to the PSTN. These Dial Patterns are then added to the Routing Policy created above.

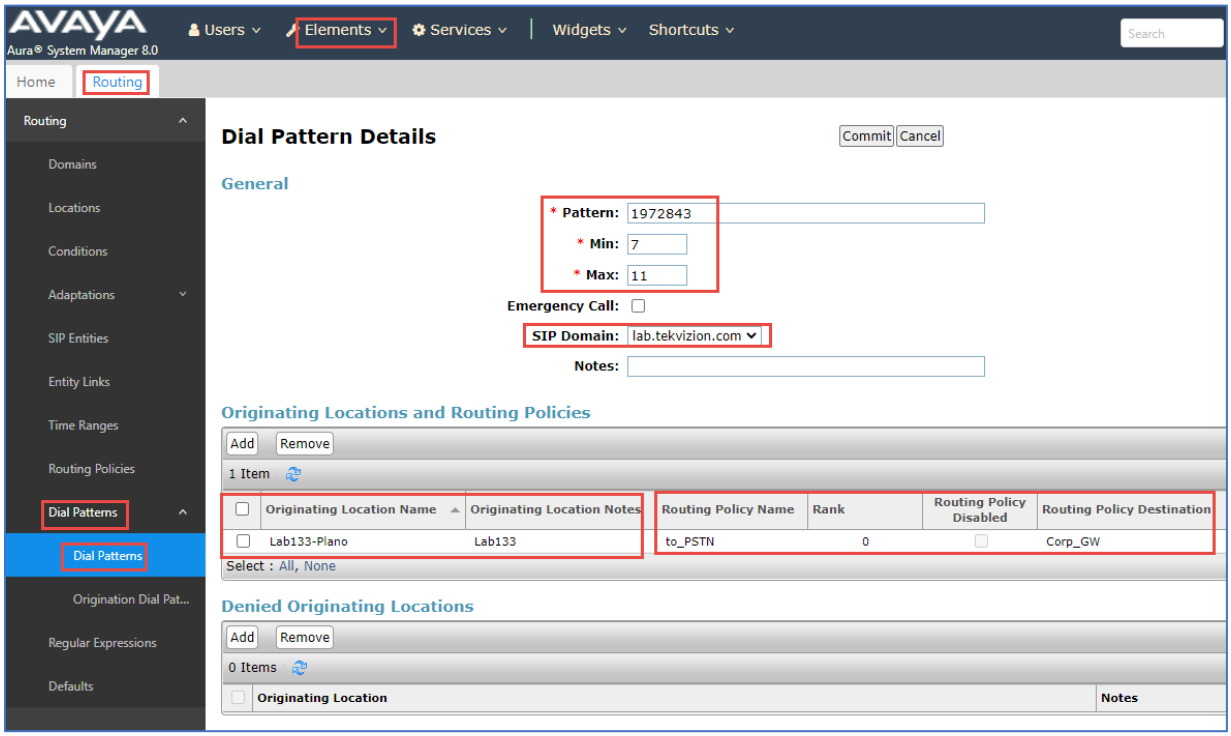
PSTN Dial Patterns

If using a SIP Trunk to the PSTN Gateway, two Dial Patterns are created one for the PSTN phone and the 2nd to the Toll-Free numbers. To add a Dial Pattern, navigate to **Elements -> Routing -> Dial Patterns.** The following are examples used for the Dial Pattern.

PSTN phone

1. Click **New**.
2. **Pattern: 1972843**.
3. **Min: 7** Minimum digits.
4. **Max: 11** Maximum digits.
5. **SIP Domain: lab.tekvizion.com** domain of the Avaya Aura.
6. **Origination Locations and Routing Policies:**
   - **Origination Location**: The location of the Avaya Aura **Lab133-Plano**.
   - **Routing Policies:** The Routing Policy to the PSTN **to_PSTN**.

Avaya Aura Session Manager: Dial Pattern: 1972843

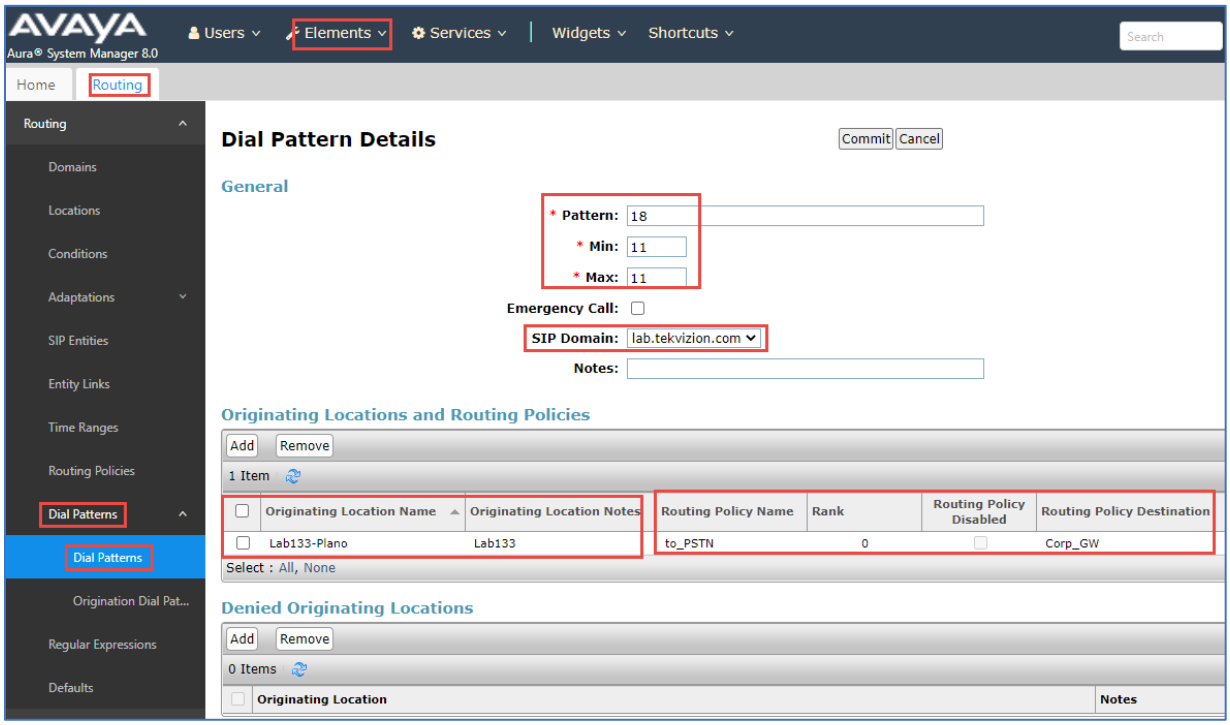


Toll-Free phone

The following are examples used for the Dial Pattern.

1. Click **New.**
2. **Pattern: 18**.
3. **Min: 11** Minimum digits.
4. **Max: 11** Maximum digits.
5. **SIP Domain: lab.tekvizion.com** domain of the Avaya Aura.
6. **Origination Locations and Routing Policies:**
   - **Origination Location**: The location of the Avaya Aura **Lab133-Plano**.
   - **Routing Policies:** The Routing Policy to the PSTN **to_PSTN**.

Avaya Aura Session Manager: Dial Pattern: 18



Avaya Aura Utility Services

The Avaya phones must be configured in the Administration settings to use the Group Procedure “2” in the 46xxsettings.text file for Secure TLS Transport between the phones and the Avaya Aura SM.

MEDIAENCRYPTION (SRTP)

To enable SRTP on the Avaya SIP phones, set the **Group_2** settings to **1** and **2** in the **MEDIAENCRYPTION** value in **46xxsettings.txt** in the IP Phone Setting editor. When the file is uploaded to the Avaya phones, the phones are configured with TLS Secure SIP and SRTP.

1. From the Avaya Aura Utility Services, change the **Group_2** settings **MEDIAENCRYPTION** to **1,2** setting **1 = aescm128-hmac80** and **2 = aescm128-hmac32.**
2. From the Avaya Aura Utility Services, the **Group_2** settings **SIPCONFERENCECONTINUE** are set to **1 – Continue conference**. This allows the conference call to stay connected after the Avaya PBX phone Conference leader drops from the call.
3. From the Avaya phone password protected **Admin Procedure** select **Group Procedure** and enter **2.** When the phone is restarted it is programed with the TLS Transport and SRTP settings.

46xxsettings.txt file

Avaya Aura Utility Services: 46xxsettings file

	GROUP_2	
☑	**SIPDOMAIN**	lab.tekvizion.com
☑	**SIP_CONTROLLER_LIST**	10.89.33.7:5061;transport=tls
☑	**CONFIG_SERVER**	10.89.33.7
☑	**SIPPROXYSRVR**	10.89.33.7
☑	**TLSSRVRID**	0 - No certificate match is necessary.
☑	**ENABLE_PPM_SOURCED_SIPPROXYSRVR**	0 - Ignore any SIP proxy address specified by PPM
☑	**TRUSTCERTS**	Lab133SMGRRoot.txt,av_prca_pem_2033.txt,av_sipca_
☑	**SUBSCRIBE_SECURITY**	0 - Use SIP addresses
☑	**ENFORCE_SIPS_URI**	0 - No
☑	**MYCERTKEYLEN**	2048
☑	**SIPSIGNAL**	2 - TLS over TCP
☑	**DIALPLAN**	[6]xxx|91xxxxxxxxxx|9[2-9]xxxxxxxxx|900xxxxxxxxxxx|
☑	**MEDIAENCRYPTION**	1,2
☑	**ENFORCE_SIPS_URI**	0 - No
☑	**ENABLE_G711A**	1 - Enable G711A
☑	**ENABLE_G711U**	1 - Enable G711U
☑	**ENABLE_G729**	1 - Enable G729A
☑	**SIPCONFERENCECONTINUE**	1 - Continue conference.

Communication Manager Messaging -CMM

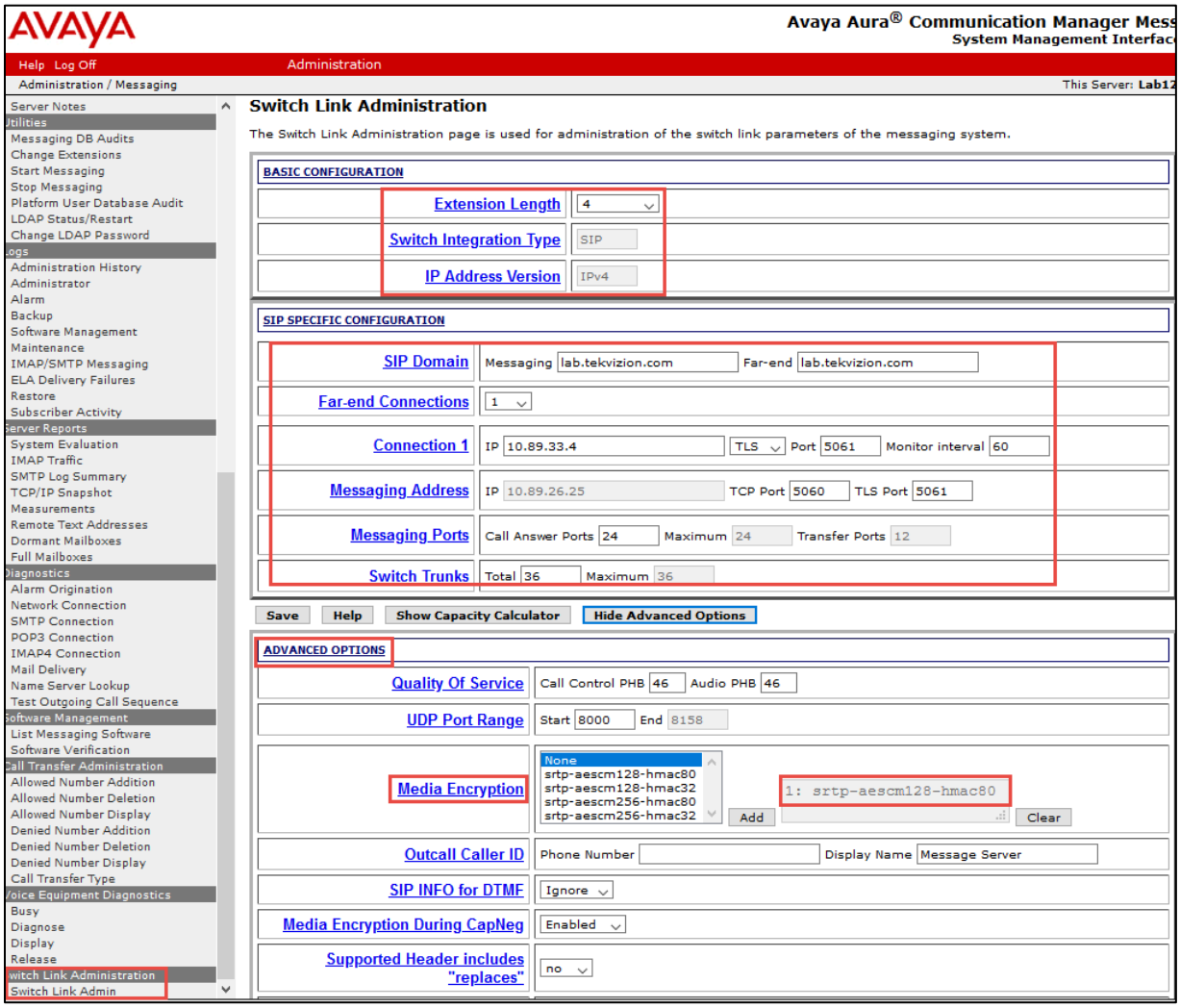
This section describes the steps for configuring the Avaya Communication Manager Messaging to interoperate with Avaya Aura Session Manager via SIP Trunking.

Switch Link Administration

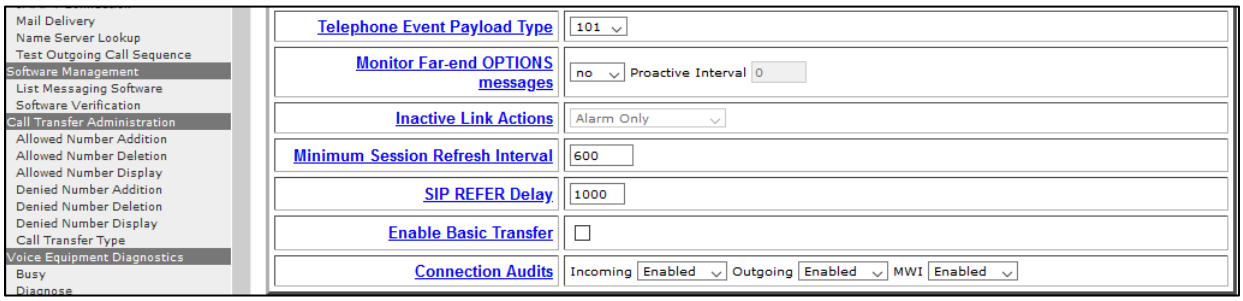
Navigate to **Administration → Messaging → Switch Link Administration → Switch Link Admin.** The following are examples used for the Link.

1. **Extension Length**: **4**.
2. In **Advanced Options**: set **Media Encryption** to **srtp-aescm128-hmac80.**
3. **Connection 1**: **10.89.26.4**, Avaya Communication Manager IP.
4. **TLS** Transport with **Port 5061**.
5. **Messaging Address**: **10.89.26.25** (Address of the CMM) **TCP Port 5060**, **TLS Port 5061.**

Avaya Aura Communication Manager Messaging: Switch Link Admin



Avaya Aura Communication Manager Messaging: Switch Link Admin (Continued)

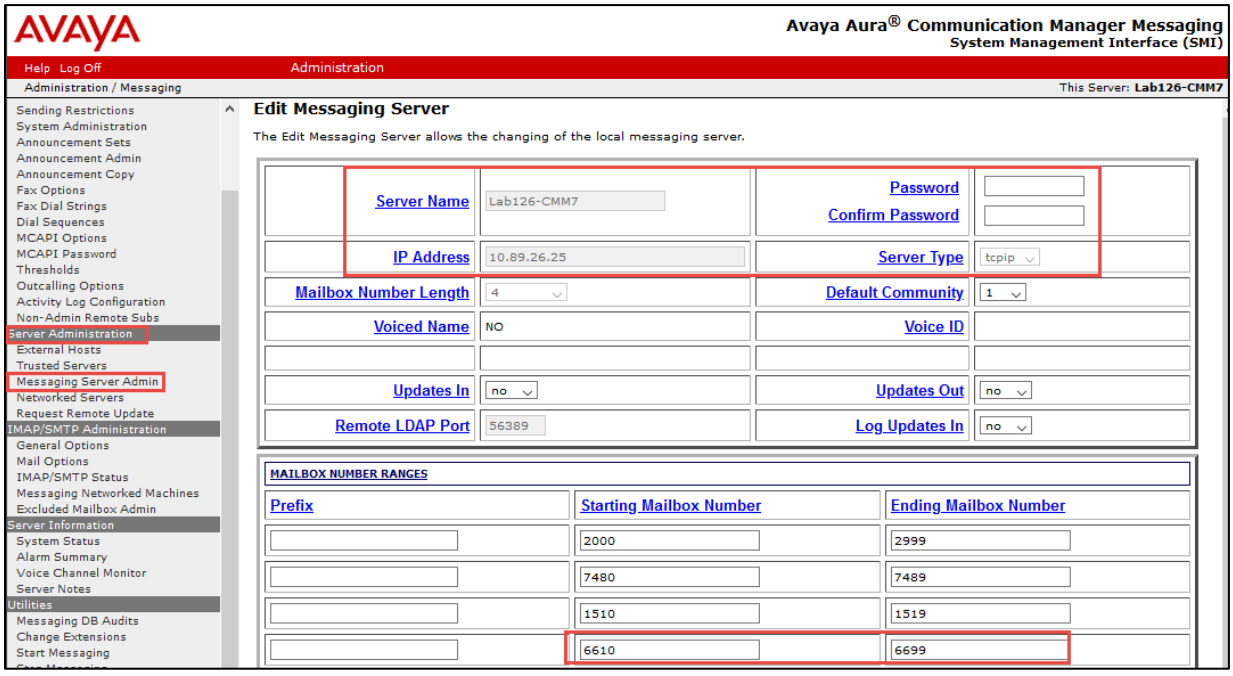


Messaging Server

To configure the parameters for the Communication Manager Messaging Server, Navigate to **Administration → Messaging →Server Administration → Messaging Server Admin.** The following are examples used for the Messaging Server.

1. **Server Name**: **Lab126-CMM7**.
2. **IP Address**: **10.89.26.25**.
3. **Starting Mailbox Number**: **6610**.
4. **Ending Mailbox Number**: **6699**.

Avaya Aura Communication Manager Messenger: Messaging Server Admin



Subscriber

To create a subscriber of the messaging server, navigate to: **Administration → Messaging →Messaging Administration → Subscriber Management.** The following are examples used for the Local Subscriber.

1. Click **Add.**
2. **Last Name**: **Mercury 1**.
3. **Mailbox Number**: **6637**.
4. **MWI Enabled**: **yes**, (Crestron Mercury phone does not support MWI).
5. Leave all other fields with their default values.

Avaya Aura Communication Manager Messenger: Subscriber Management