CCS-UC-1

Secure SIP Endpoint with Avaya Aura® 7.0 System

Configuration Guide

Crestron Electronics, Inc.

This document was written by the Technical Publications department at Crestron.

Contents

CCS-UC-1: Secure SIP Endpoint with Avaya® Aura 7.0

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.

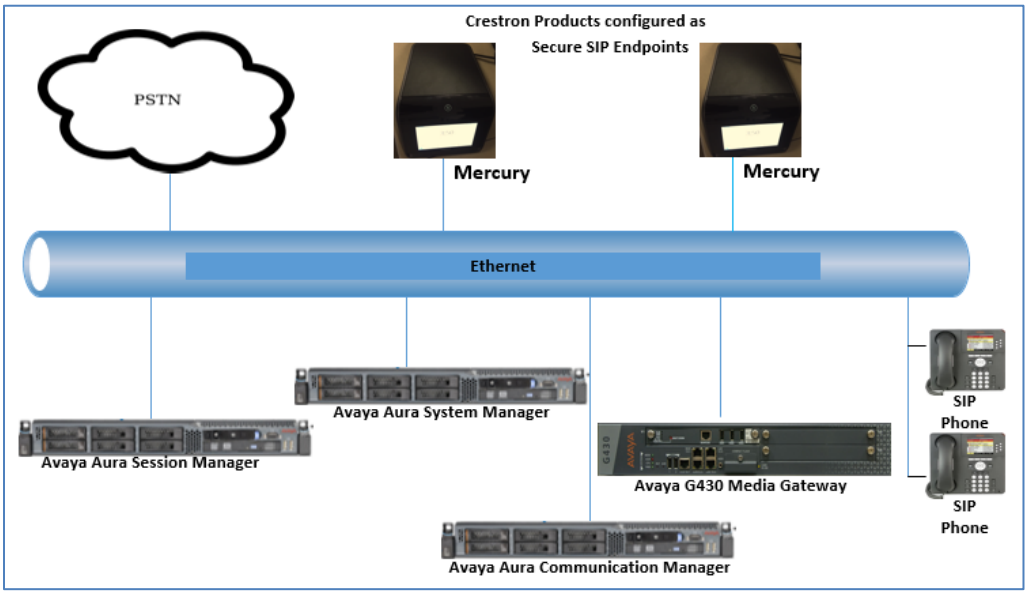
Audience

This document is intended for users attempting to configure and use Crestron Mercury devices as secure SIP endpoints registering to the Avaya Aura Communication Manager.

Topology

The network topology for the Crestron Mercury endpoint to interop with the Avaya Aura is shown below.

Crestron Mercury: Secure 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 SIP phones
- Avaya G430 Media Gateway
- Crestron Mercury device as the secure SIP Endpoints

Software Requirements

- Avaya Aura Communication manager v 7.0.1.1.0.441.23169
- Avaya Aura System Manager v 7.0
- Avaya Aura Session Manager v 7.0.1.1.701114
- Avaya g430 Media Gateway v 37 .39 .0 /2
- Crestron Mercury devices v 1.3318.00002 and v 1.3318.00013.001(G729 testing)

Hardware Requirements

- Avaya components either in a virtual environment or separate hardware servers
    - Avaya Aura Communication Manager
    - Avaya Aura Session Manager
    - Avaya G430 Media Gateway
    - Avaya Aura Session Manager
- PRI Gateway for PSTN Calling
- Avaya phones (3) in SIP mode
- Crestron Mercury devices (2)

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® product for conference rooms that integrates microphones and speakers into the user interface at the table.

Crestron Toolbox™ software is used to discover and control all Crestron devices on the network.

The Crestron Mercury web Interface is used to control the Crestron Mercury devices on the network.

Summary

The Crestron Mercury devices, in secure mode, are configured on the Avaya Aura as SIP endpoints. The devices successfully register to the Avaya Aura Session Manager with digest authentication after establishing a TLS connection with the PBX.

Features Supported

- Secure mode: Establishing a TLS handshake with the Avaya Aura
- Registration with Digest Authentication
- Basic Calls with G729, G722, G711u, and G711a codecs
- Caller ID (limited to only calling number)
- DTMF support
- Early media support
- Retrieval of a parked call
- Transferee in a call transfer
- Conference participant
- Member of hunt group

Features Not Supported

- Caller ID presentation
- Call hold and resume
- Call forwarding on the device (Forwarding can be configured on the PBX for the DN assigned to the endpoint)
- Call waiting
- Conference
- Attended call transfer
- Early attended call transfer
- Blind call transfer
- Shared line (configuration of shared line on device)
- Call park (initiating call park)
- Message waiting indicator

Known Issues/Limitations

- The “Direct IP-IP Audio Connections” parameter on the Avaya Aura signaling group was configured to “n” (No) instead of the default value of “y” (Yes) because with it set to “y,” the CM would reject a call made by an Avaya phone to the Crestron Mercury device.
- Caller ID is not supported on Crestron Mercury devices. Currently only the calling party number is displayed as the caller ID. This issue is tracked via Crestron’s Bugzilla™ software Defect: 119006.
- The active call timer on the Crestron Mercury device does not reflect the correct call duration. The active call duration includes the time for which the unit was being alerted also. This issue is tracked via Crestron’s Bugzilla software Defect: 124001.

- The first ringback heard on the Crestron Mercury device is stuttered (resembles a mix of local and remote ringback). This issue is tracked via Crestron's Bugzilla software Defect: 122421.
- On the Crestron Mercury web user interface, there is currently no notification provided to the user when certain configurations are missing. This issue is tracked via Crestron's Bugzilla software Defect: 125193.
- On the Crestron Mercury web user interface, a configuration of DHCP OFF on the Network configuration page mandates configuration of both the adapters. The user is unable to save changes unless both the adapters are configured and is notified of an invalid IP against the default of 0.0.0.0 for an unused adapter. This issue is tracked via Crestron's Bugzilla software Defect: 126236.
- On the Crestron Mercury web user interface, there is currently no check to validate if a certificate that is being deleted is in use or not, i.e., whether it is on the trusted list or not. This issue is tracked via Crestron's Bugzilla software Defect: 126232.
- On the Crestron Mercury device, for certain called numbers that cannot be reached or are invalid, the user only hears a reorder tone and does not have the option to disconnect the call except by pressing the call button again. This issue is tracked via Crestron's Bugzilla software Defect: 122633.

Crestron Mercury Configuration

Setup

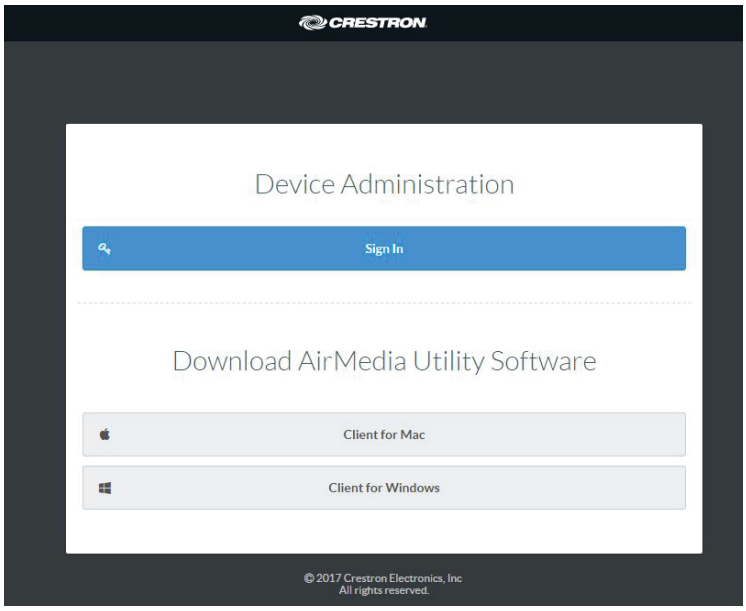
The LAN port of the Crestron Mercury device needs to be connected to one PoE+ port to power it up for network connectivity with the Avaya Aura. The PoE switch that is used should have the LLDP functionality enabled for the device to power up and be completely functional. By default the "poeplus" configuration is set to Off on the device.

Configuring the device

To configure the device, follow this procedure:

1. Access the web GUI for the device by using an http session with the device's IP address. The device IP address used in this test was *10.89.17.100*.

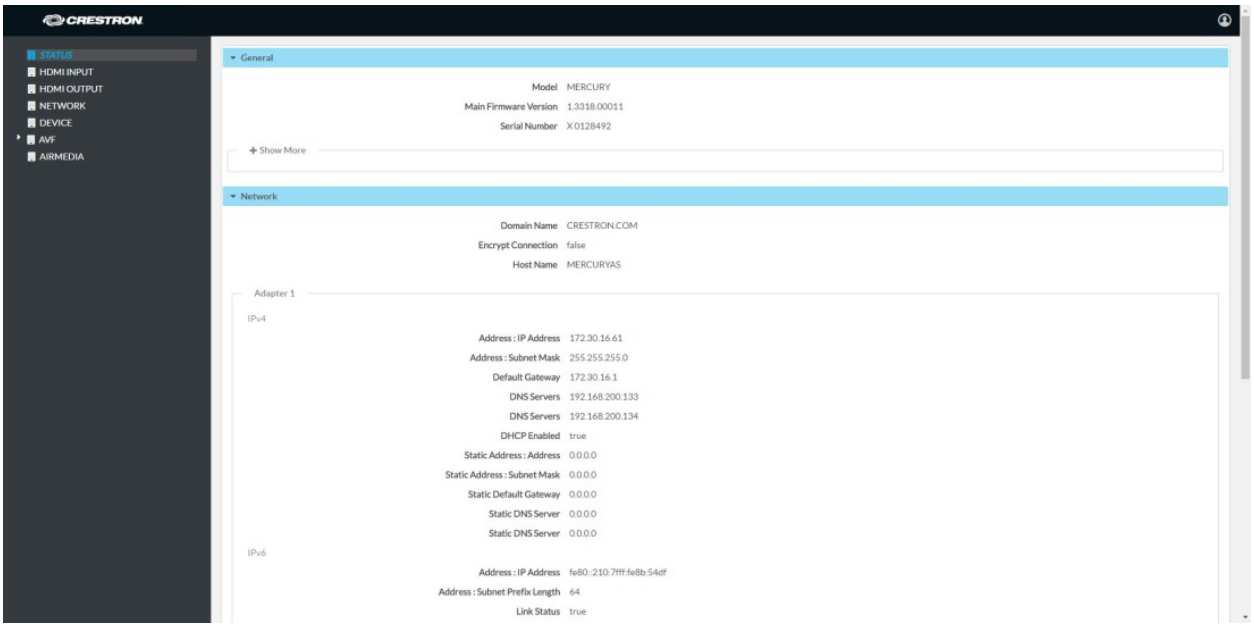
Crestron Mercury: Login to Web GUI



2. Click **Sign In** and log in to the device. For information on device administration, refer to the CCS-UC-1 Supplemental Guide (Doc. 7844) at www.crestron.com/manuals.

   The Status screen that appears displays basic information on the device.

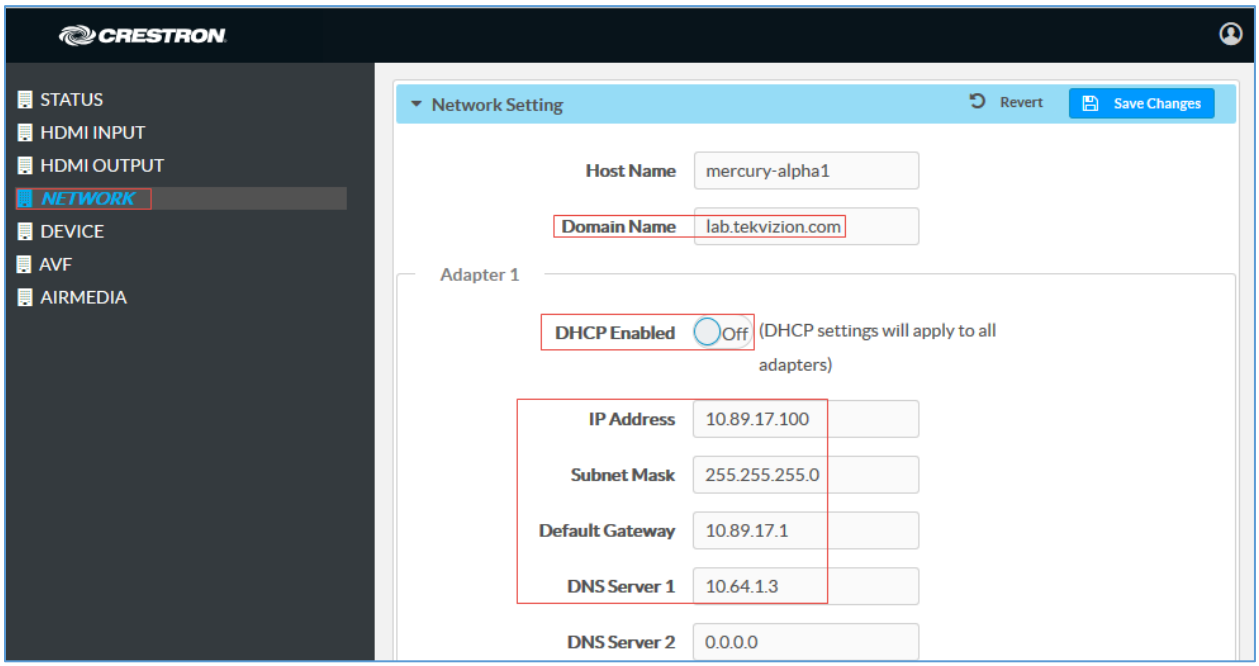
Crestron Mercury: Status



The device can be configured from the **Network** page.

3. On the web GUI, navigate to **Network**

Crestron Mercury: Network Setting: DHCP Off: Static IP Configured



4. Enter the following parameters in the **Adapter 1** section to configure the Crestron Mercury device.
   - **Domain Name**: *lab.tekvizion.com*, used in this example (mostly auto-detected by device when in DHCP mode).
   - **DHCP**: Choose either of the following:
     - Obtain an IP address automatically
     - Use the following IP address

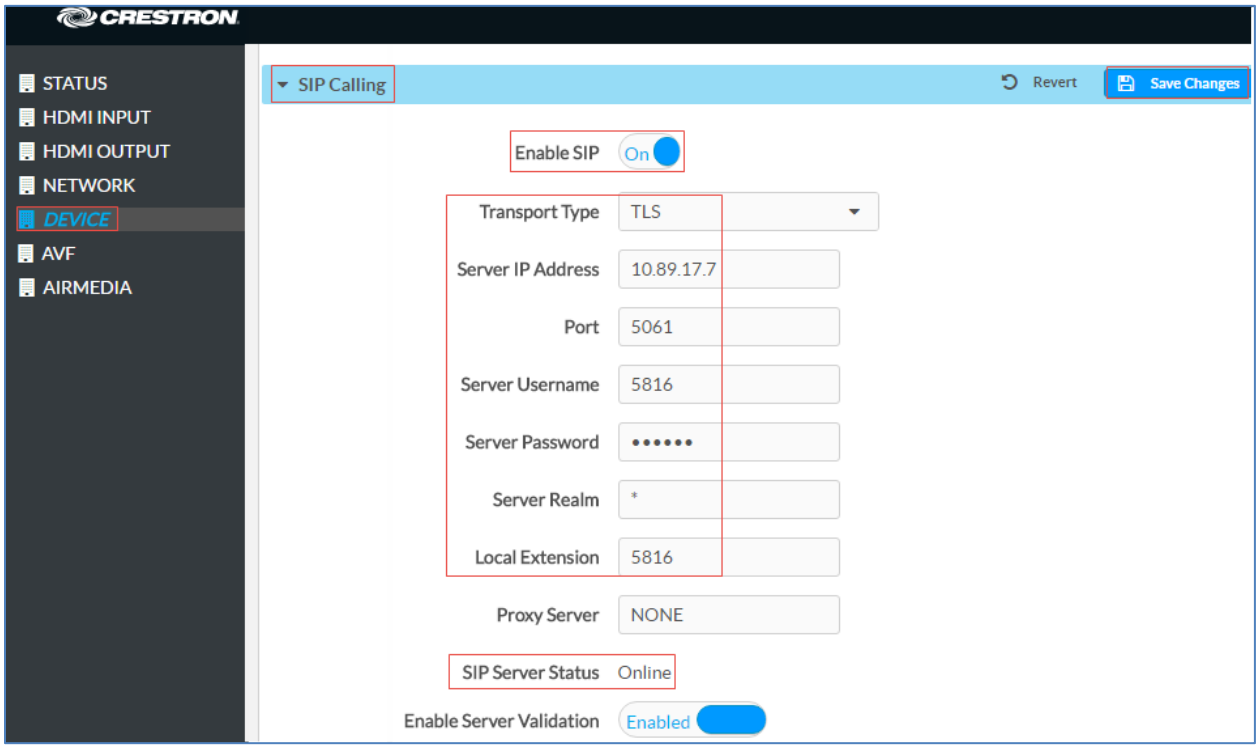
     For the test, a static IP was configured.
       - **IP address**: *10.89.17.100* was used in this example.
       - **Subnet Mask**: *255.255.255.0* was used in this example.
       - **Default Gateway**: *10.89.17.1* was used in this example.
       - **DNS Server 1**: *10.64.1.3* was used in this example.
5. Click **Save Changes**.

Configure the TLS SIP Parameters

To configure the TLS SIP parameters, follow this procedure:

1. On the web GUI, navigate to **Device** > **SIP Calling**.

Crestron Mercury: Device Configuration: TLS SIP Parameters



2. Enable the check box for **Enable SIP**.
3. Configure the **Server IP Address:** Enter the IP address of the Avaya Aura Session Manager node. *10.89.17.7* was used in this example.
4. Configure the **port**: *5061*, used in this example.
5. Configure the **Server Username**: Enter the end user configured on Avaya Aura Communication Manager for this device. *5816* was used in this example.
6. Configure the **Server Password**: Enter the password as configured on Avaya Aura Communication Manager for this end user.
7. Configure the **Local Extension**: Enter the directory number that was configured for this device on Avaya Aura Communication Manager. *5816* was used in this example.
8. Leave all other fields at their default values.
9. Click **Save Changes**.

Once the device successfully registers with the Avaya Aura Session Manager, the **SIP Server Status** updates its status to show *Online.*

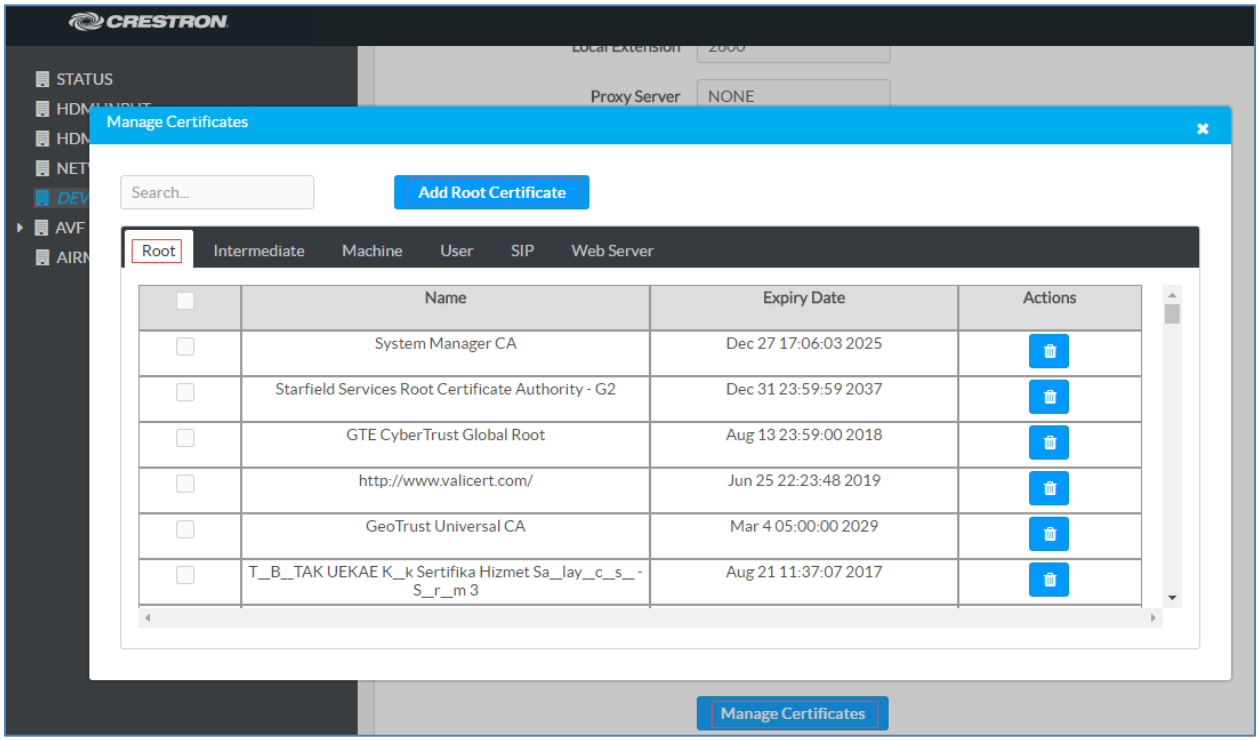
Add certificates

For a successful TLS handshake with the Avaya Aura Session Manager, the Crestron Mercury device 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 device to allow it to validate the Avaya Aura Session Manager when Enable Server Validation is enabled in the SIP Calling configuration screen.

Perform the following procedure to upload certificates to the Crestron Mercury device.

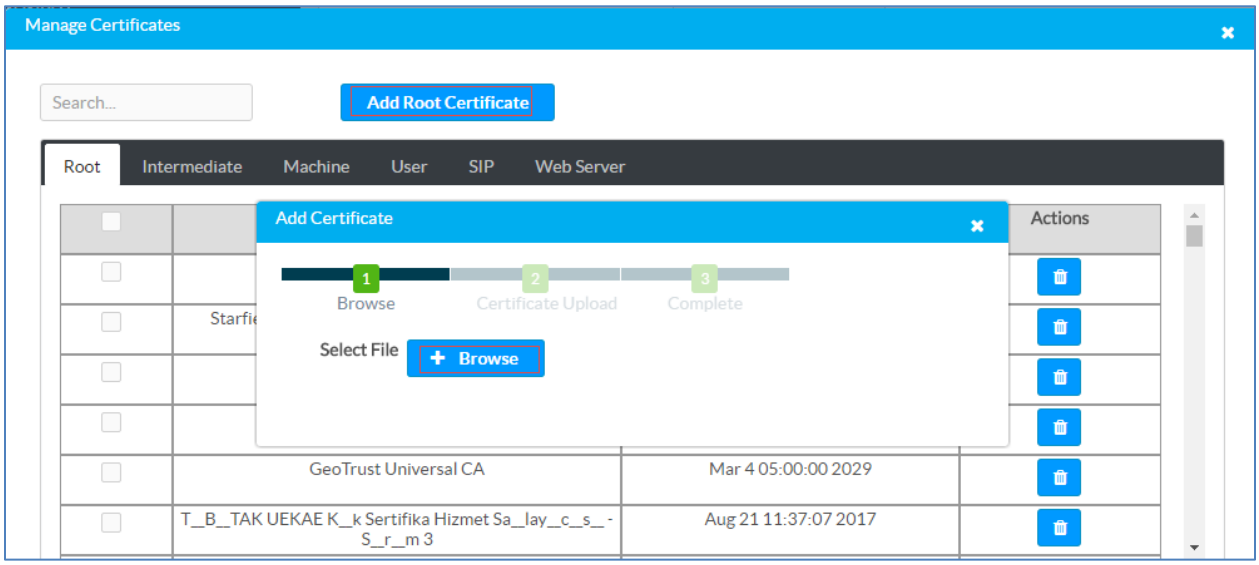
1. On the web GUI, navigate to Device > SIP Calling.
2. Click Manage Certificates.

Crestron Mercury: Manage Certificates: Add Root Certificate



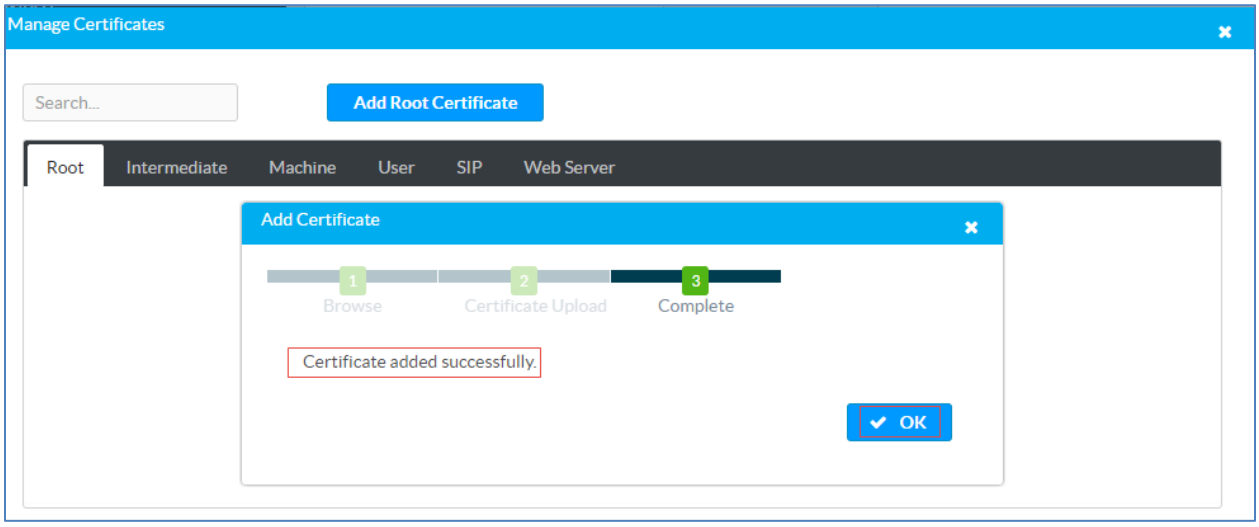
3. Click Add Root Certificate.

Crestron Mercury: Manage Certificates: Add Root Certificate: Browse



4. In the **Add Certificate** window, click **Browse**.
5. Select the *root_cer.cer* file that needs to be uploaded, and click **Ok**.
6. On the screen that follows, click **Load**. The device indicates that the certificate was added successfully.

Crestron Mercury: Manage Certificates: Add Root Certificate: Add Complete

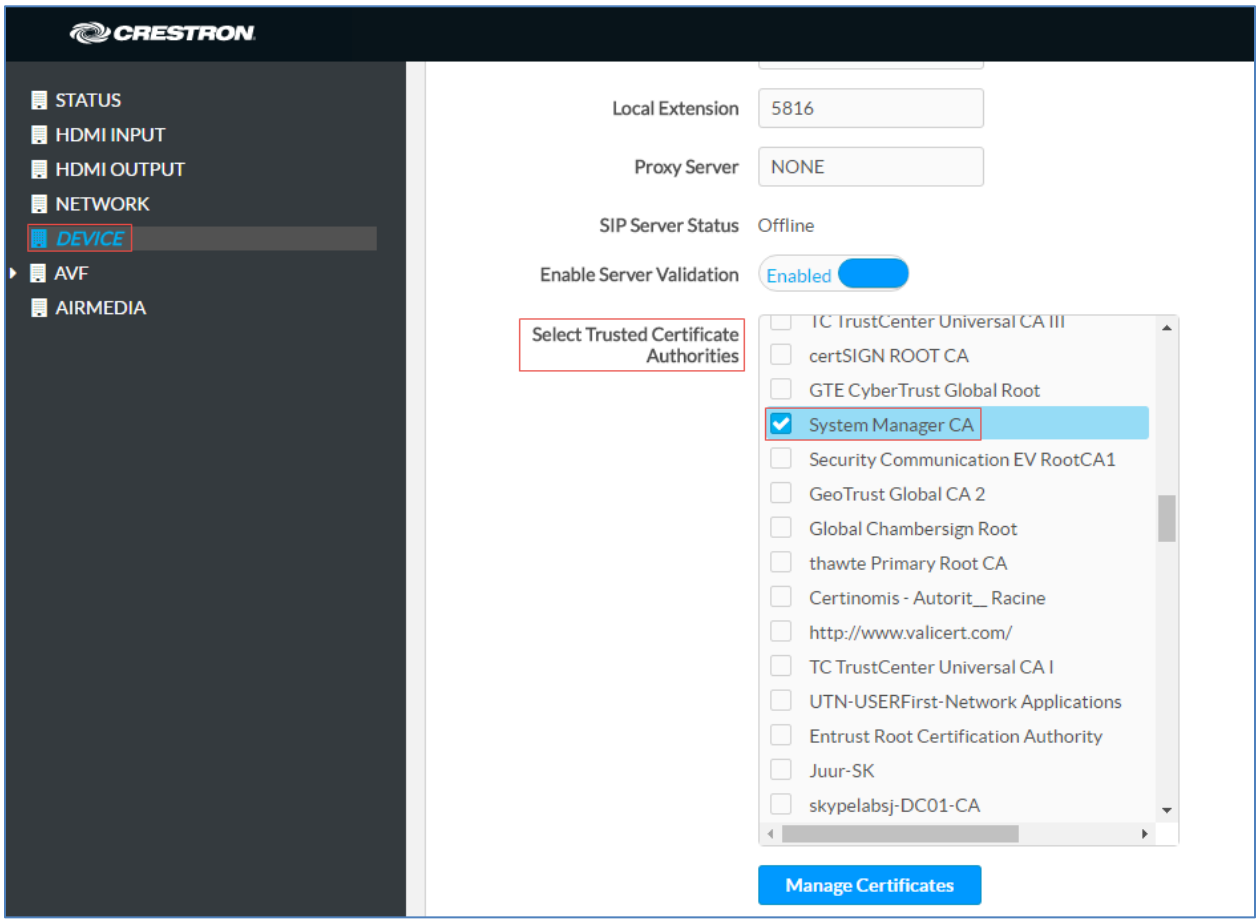


7. Click **OK** and close the **Manage Certificates** window.

   The certificate authority from where this root-cer certificate was downloaded appears in the list of trusted certificate authorities.

8. On the main **SIP Calling** screen, navigate to **Select Trusted Certificate Authorities**.

Crestron Mercury: SIP Calling: Select Trusted Certificate Authorities



9. From the list of certificate authorities, select the certificate authority (from where the *root_cer.cer* certificate was downloaded).

Avaya Aura Communication Manager Configuration

This section describes the Avaya Aura Communication Manager (Avaya CM) configuration necessary to support the registration of the devices in a secure mode, and connectivity to PSTN.

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 name-names ip command to add the node name. In this example, *procr* and *ASM7* were added with their respective IPs.

- *ASM7* is an Avaya Aura Session Manager used in this example and is used to register the SIP phones and third-party SIP devices.
- *procr* is used to register the SIP trunk.

Avaya Aura CM: Configure Node

```
display node-names ip
                                    IP NODE NAMES
    Name                 IP Address
ASM7                   10.89.17.7
CMM7                   10.89.17.25
default                0.0.0.0
procr                  10.89.17.4
procr6                 ::

( 5  of 5    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

Command:
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.

For the test, **ip-codec-set 1** was configured with the following codecs supported by the Crestron Mercury device: **G722**, **G711MU**, **G.711A**, and **G729**.

Avaya Aura CM: Codec Configuration

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

                         IP CODEC SET
   Codec Set: 1

   Audio        Silence      Frames   Packet
   Codec        Suppression  Per Pkt  Size(ms)
1: G.729             n         2        20
2: G.711MU           n         2        20
3: G.722-64K                   2        20
4: G.711A            n         2        20
5:
6:
```

Network Region

Configure an IP Network region 1 using the **change ip-network-region 1** command.

To configure an IP Network region, issue the above command and configure:

- Set **Authoritative Domain**: *lab.tekvizion.com*, used in this example
- Set **Name**: provide any relevant name.
- **Codec Set**: *1*, which is programmed in the previous step.
- **Set Intra-region IP-IP Direct Audio**: *Yes*.
- **Set Intra-region IP-IP Direct Audio**: *Yes*.
- Retain all other default configurations.

Avaya Aura CM: IP Network Region Configuration

```
change ip-network-region 1                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: lab.tekvizion.com
   Name:                        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? n
   UDP Port Max: 65535
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
```

Signaling Group

For this test, two signaling groups were configured:

- *signaling-group 1* for calls between the Communication Manager and Session Manager
- *signaling-group 10* for PSTN calls

Using the command **add signaling-group 1**, add and configure Signaling Group 1 as follows:

- **Group Number:** *1*, used in this example.
- **Group Type:** *sip*, used in this example.
- **Transport Method:** *tls*, used in this example.
- **Near-end Node Name:** *procr*, used in this example.
- **Near-end Listen Port:** *5061*, used in this example.
- **Far-end Node Name:** *ASM7*, used in this example.
- **Far-end Listen Port:** *5061*, used in this example.
- **Far-end Network Region:** *1*, used in this example.
- **Far-end Domain:** *lab.tekvizion.com,* used in this example.
- **DTMF over IP:** *rtp-payload*, used in this example.
- **Direct IP-IP Audio Connections?** *n*, used in this example. (There were issues with setting it to "yes." The CM would reject a call made by an Avaya phone to the Crestron Mercury device.)

Avaya Aura CM: Signaling Group Configuration: CM to SM Calls

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

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? n        Enforce SIPS URI for SRTP? n
  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: procr                 Far-end Node Name: ASM7
 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
```

Using the command **add signaling-group 10**, add and configure the Signaling Group 10 as follows:

- **Group Number:** *10*, used in this example.
- **Group Type:** *isdn-pri*, used in this example.
- **Associated Signaling?:** *y*, used in this example.
- **Primary D-Channel:** *001V224*, used in this example.
- **Trunk Group for Channel Selection:** *10*, used in this example.

Avaya Aura CM: Signaling Group Configuration: CM to PRI GW

```
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: 001V224     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
```

Trunk Groups

Two trunk groups were configured for this test:

- Trunk Group 1 utilized a private numbering plan to access the stations registered to the Avaya Session Manager.
- Trunk Group 10 utilized a public numbering plan to send place PSTN calls via a PRI GW.

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

Configure Trunk Group 1:

- Group Number: *1*, used in this example.
- Group Name: *SIP Phone*, used in this example.
- Group Type: *sip,* used in this example.
- Service Type: *tie*, used in this example.
- TAC: *#001*, used in this example.
- Signaling Group: *1*, used in this example.
- Number of Members: *10*, used in this example.
- Preferred Minimum Session Refresh Interval (sec): *600*.
- Numbering Format: *private*.

Avaya Aura CM: Trunk Configuration to Session Manager (1/4)

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

Group Number: 1                 Group Type: sip          CDR Reports: y
  Group Name: SIP Phone                 COR: 1        TN: 1        TAC: #001
   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: 10
```

Avaya Aura CM: Trunk Configuration to Session Manager (2/4)

```
display trunk-group 1                                          Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                          Redirect On OPTIM Failure: 5000

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

Avaya Aura CM: Trunk Configuration to Session Manager (3/4)

```
display trunk-group 1                                          Page   3 of  21
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
```

Avaya Aura CM: Trunk Configuration to Session Manager (4/4)

```
display trunk-group 1                                          Page   4 of  21
                              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? 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: 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
```

Configure Trunk Group 10:

- Group Number: *10*, used in this example.
- Group Name: *OUTSIDE CALL*, used in this example.
- Group Type: *isdn*, used in this example.
- Carrier Medium: *PRI/BRI*, used in this example.
- TAC: *#010*, used in this example.
- Numbering Format: *private*.

Avaya Aura CM: Trunk Configuration to PRI GW (1/3)

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

Group Number: 10              Group Type: isdn          CDR Reports: y
  Group Name: OUTSIDE CALL          COR: 1        TN: 1        TAC: #010
   Direction: two-way     Outgoing Display? y     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
```

Avaya Aura CM: Trunk Group 10 Configuration for PSTN PRI dialing (2/3)

```
display trunk-group 10                                          Page   2 of  21
      Group Type: isdn

TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
        Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: a     Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: cyclical
                                                   Digital Loss Group: 13
Incoming Calling Number - Delete:     Insert:                 Format:
              Bit Rate: 1200         Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0
          Administer Timers? n        CONNECT Reliable When Call Leaves ISDN? n
             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n





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

Avaya Aura CM: Trunk Group 10 Configuration for PSTN PRI dialing (3/3)

```
display trunk-group 10                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none      Wideband Support? n
                                                          Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                      Send Name: n      Send Calling Number: n
            Used for DCS? n                            Send EMU Visitor CPN? n
   Suppress # Outpulsing? n
 Outgoing Channel ID Encoding: preferred     UUI IE Treatment: service-provider

                                                  Replace Restricted Numbers? n
                                                 Replace Unavailable Numbers? n
                                                       Send Connected Number: n
Network Call Redirection: none                     Hold/Unhold Notifications? n
             Send UUI IE? y
               Send UCID? n
 Send Codeset 6/7 LAI IE? y                          Ds1 Echo Cancellation? n

    Apply Local Ringback? n                US NI Delayed Calling Name Update? n
 Show ANSWERED BY on Display? y      Invoke ID for USNI Calling Name: variable
                              Network (Japan) Needs Connect Before Disconnect? n
```

Inbound Routing

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

For the test, a DID starting with 972852269x was used. The **inc-call-handling-trmt** on the trunk group 10 (used to route the internal calls) was configured to delete the first 9 digits and prefix a 581 to reach the 581x four-digit extensions.

Avaya Aura CM: Inbound Routing

```
change 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 972852269        9   581
 public-ntwrk
 public-ntwrk
 public-ntwrk
```

Outbound Routing

Configure the automatic route selection, route pattern, and auto-alternative routing.

Automatic Route Selection (ARS)

The **Automatic Route Selection (ARS)** feature is used to route outbound calls via the SIP trunk to the PSTN. In the sample configuration, the single digit **9** is used as the ARS access code. PBX users dial 9 to initiate a call to PSTN. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with *9* of length *1* as a feature access code (**fac**).

Avaya Aura CM: Outbound Routing: Configure Dial Plan Analysis Table

```
change dialplan analysis                                        Page   1 of  12
                          DIAL PLAN ANALYSIS TABLE
                                Location: all            Percent Full: 2

   Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
   String   Length Type     String   Length Type     String   Length Type
  0          1    attd
  2          4    ext
  5          4    ext
  65         4    ext
  7          4    ext
  8          1    fac
  9          1    fac
  *          3    fac
  #          4    dac
```

The following feature access codes were configured for this test:

- **Auto Route Selection (ARS)**: *9* was used in this example.
- **Call Park Access Code**: **70* was used to initiate a call park.

- Answer Back Access Code: *72 was used to retrieve a parked call.

Avaya Aura CM: Outbound Routing: Configure Feature Access Codes

```
display feature-access-codes                                    Page   1 of  10
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                      Answer Back Access Code: *72

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:       Deactivation:
   Call Forwarding Enhanced Status:        Act:       Deactivation:
                        Call Park Access Code: *70
                      Call Pickup Access Code: *71
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                  Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                  Contact Closure   Open Code:          Close Code:

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

Use the change ars analysis command to configure the routing of dialed digits following the first digit 9.

For the example, the following entries were added using the above command and configuring:

- *1*: to accommodate all 18xx numbers or national numbers prefixed by a 1
- *214*, *214242*, and *972*: to accommodate the lab and generic PSTN numbers used during the example.

Avaya Aura CM: Outbound Routing: Auto Route Selection (1/2)

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

         Dialed           Total     Route    Call   Node  ANI
         String          Min  Max  Pattern   Type   Num   Reqd
   1                     11   11    10       pubu         n
```

Avaya Aura CM: Outbound Routing: Auto Route Selection (2/2)

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

         Dialed           Total     Route    Call   Node  ANI
         String          Min  Max  Pattern   Type   Num   Reqd
   2                     7    7     deny     hnpa         n
   214                   10   10    10       natl         n
   214242                10   10    10       natl         n
   411                   3    3     3        svcl         n
   911                   3    3     3        emer         n
   972                   10   10    10       pubu         n
                                                           n
```

Route Pattern

The route pattern defines which trunk group will be 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: *10* is used in this example for PSTN calls.

Grp No: *1* is used in this example.

Avaya Aura CM: Route Pattern Configuration

```
display route-pattern 10                                         Page   1 of   3
                   Pattern Number: 10     Pattern Name: PRI
   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                                      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
```

Auto Alternative Routing

Use the **change aar analysis n** command where **n** is the first digit of the extension numbers used for SIP stations in the system.

The following entries were configured for this example:

- **Dialed number**: *5*, used for Avaya SIP phones and Crestron Mercury SIP devices.
- **Dialed number**: *214*, used for PSTN numbers.

Avaya Aura CM: Modify AAR Digit Analysis Table

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

         Dialed           Total     Route    Call   Node  ANI
         String          Min  Max  Pattern   Type   Num   Reqd
   2                     4    4     4        aar          n
   214                   10   10    4        aar          n
   4                     7    7     254      aar          n
   5                     4    4     1        unku         n
   5000                  4    4     2        unku         n
```

Hunt Group

One hunt group was configured for this example:

Hunt Group Extension: *5002*, used in this example for **Group Hunt** feature.

Use the ***add hunt-group n*** to add a new hunt group where **n** is the available hunt group number.

Avaya Aura CM: Hunt Group Configuration (2/3)

```
display hunt-group 4                                            Page   1 of  60
                                  HUNT GROUP

           Group Number: 4
             Group Name: HuntGroup
        Group Extension: 5002
             Group Type: circ                  Coverage Path: 2
                     TN: 1          Night Service Destination:
                    COR: 1                   MM Early Answer? n
          Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:
```

Configure the Hunt Group:

- **Group Number:** *4* is used in this example.
- **Group Name:** *HuntGroup* is used in this example.
- **Group Extension;** *5002* is used in this example.
- **Group Type:** *circ* is used in this example to enable sequential ringing on the hunt group members.

- Coverage Path: *2* is used in this example, which includes hunt group members that will be alerted sequentially.

Use the *add coverage path n* command (where n is the available coverage path number) to add the coverage path, which includes members of the hunt group.

Coverage Path Number 2 was configured in the example. This is invoked by Hunt group 4.

The following coverage points were configured:

- Point1: *5818* is used in this example.
- Point2: *5817* is used in this example.
- Point3: *5816* is used in this example.

Avaya Aura CM: Hunt Group Coverage Path Configuration

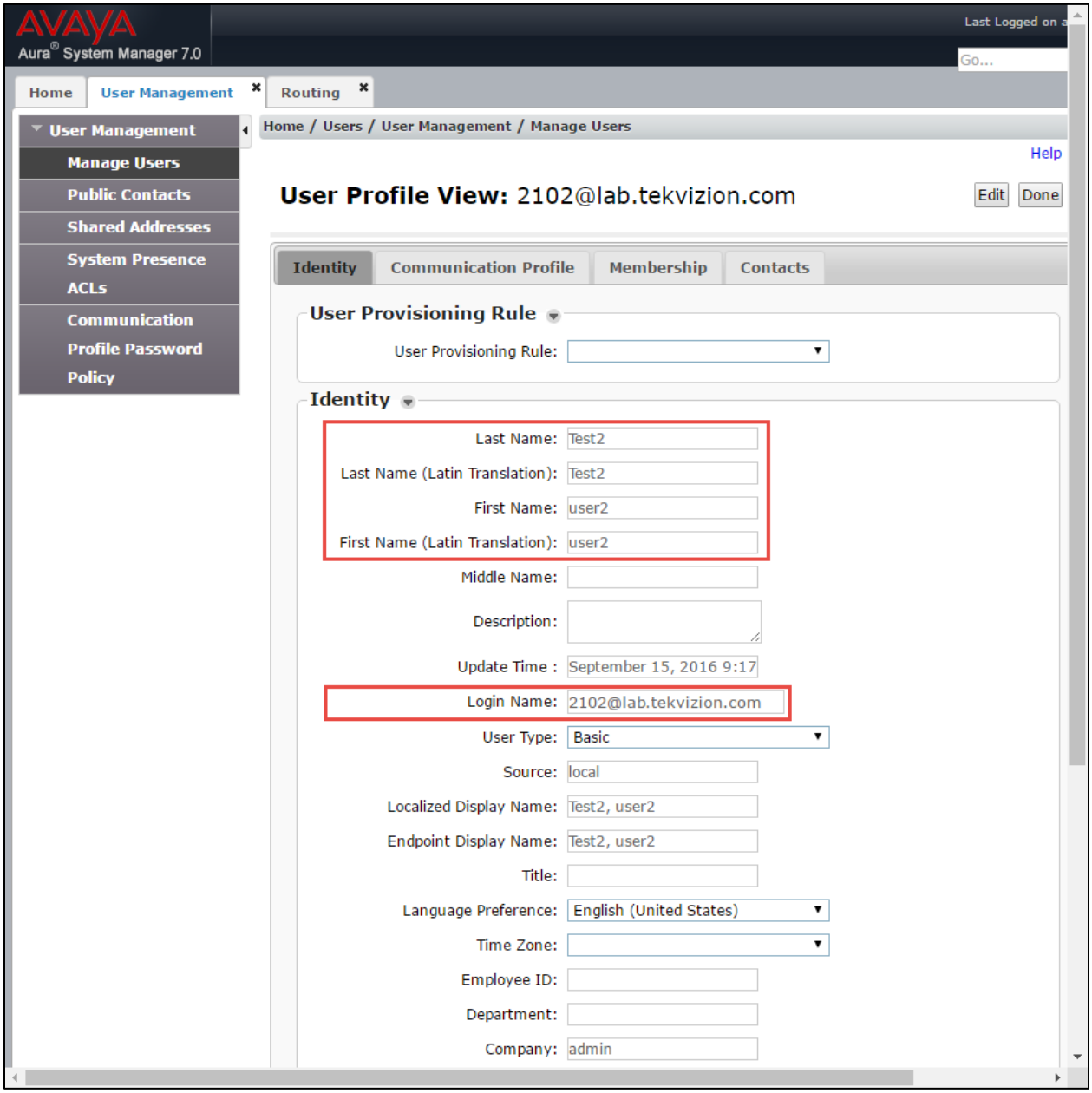
```
display coverage path 2
                                COVERAGE PATH

                   Coverage Path Number: 2
     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: 5818           Rng: 2  Point2: 5817           Rng: 3
  Point3: 5816           Rng:    Point4:
  Point5:                        Point6:
```

Configuring a User for Each Device/Phone

A user was configured for each phone or Crestron device used in the example. To configure a user for each device/phone, follow this process:

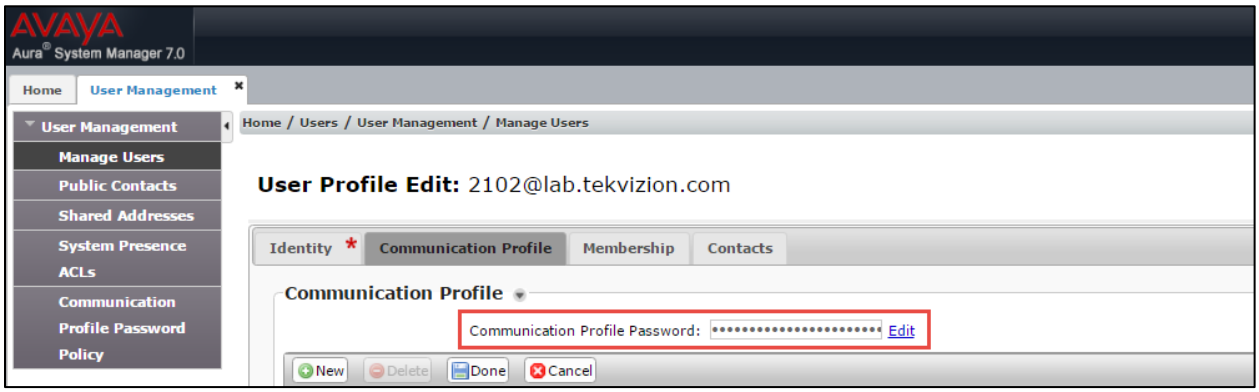
1. Navigate to **Home** > **User Management** > **Manage Users**.
2. Click **Add New**. The User Profile configuration window appears.

Avaya Aura CM: Phone Configuration (1/4)



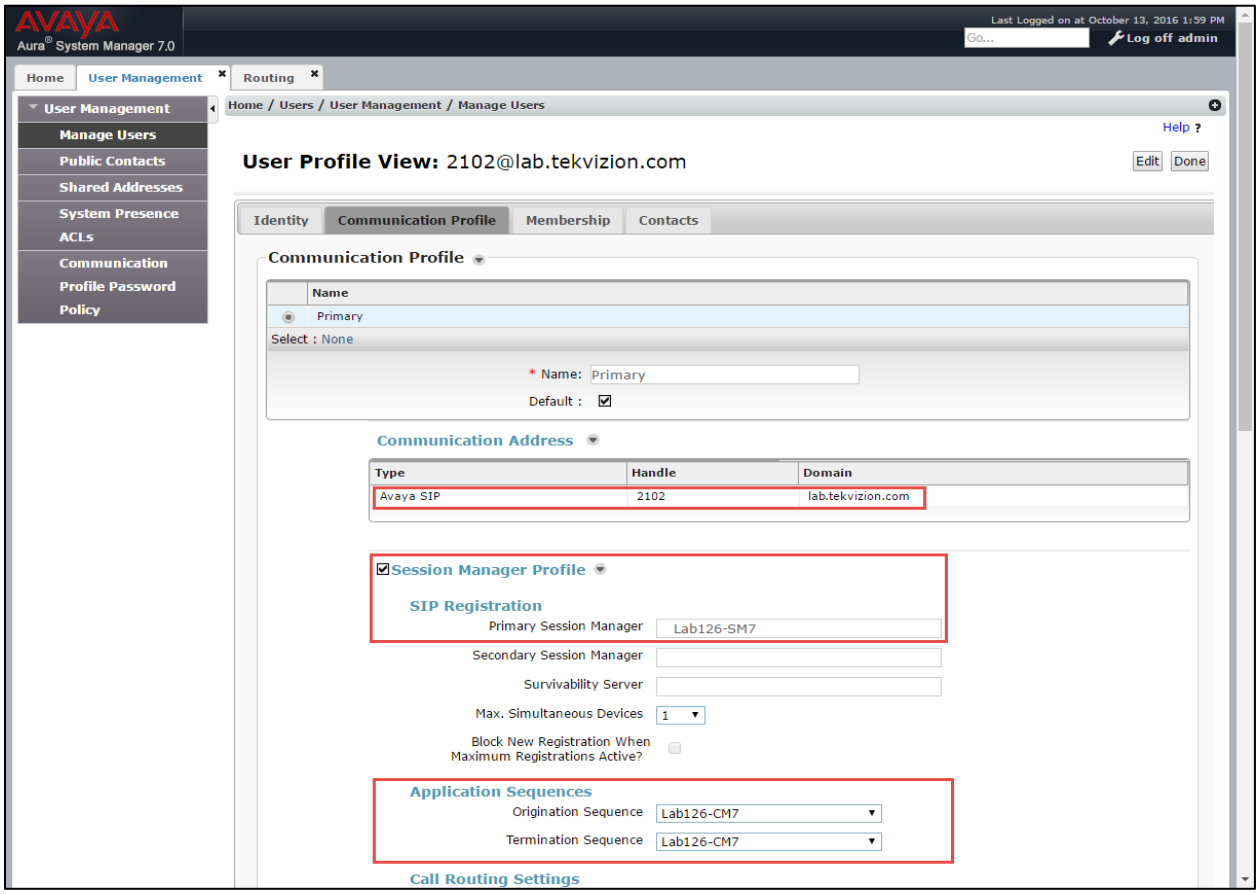
3. Configure **Last Name** and **First Name:** *Test.2*, used in this example.
4. Configure **Login Name:** *2102@lab.tekvizion.com*, is used in this example.
5. Select **Communication Profile** tab.

Avaya Aura CM: Phone Configuration (2/4)



6. Configure **Communication Profile Password:** enter the desired password for the SIP user to use for registration.
7. Confirm Password.
8. Scroll down to Communication Address subsection, and click **New** to add a new address.

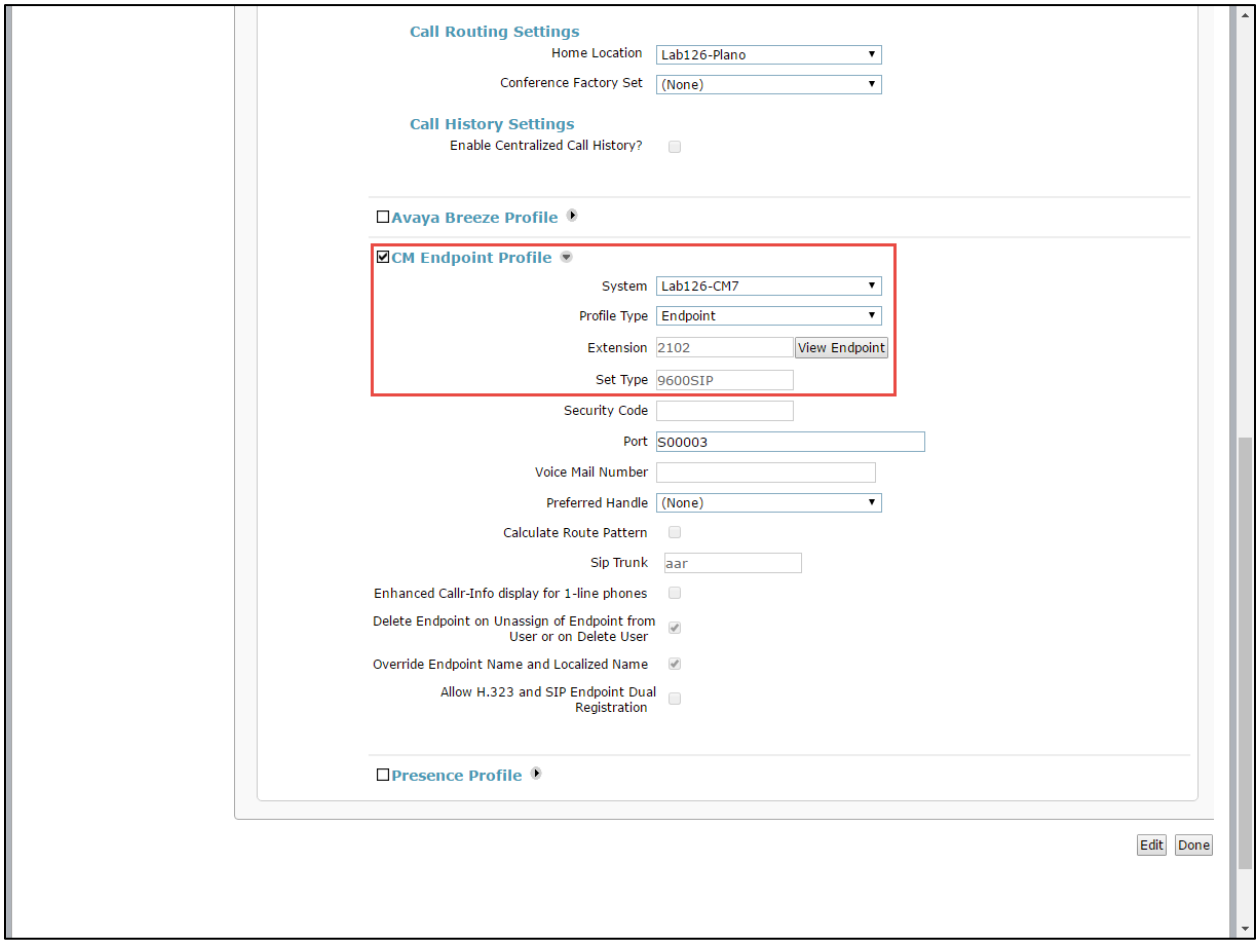
Avaya Aura CM: Phone Configuration (3/4)



9. Configure **Communication Manager Type:** Avaya SIP.

10. Enter **SIP Registration:** Primary Session Manager. *Lab126-CM7*, used in this example.
11. Check the **CM Endpoint Profile** check box.

Avaya Aura CM: Phone Configuration (4/4)

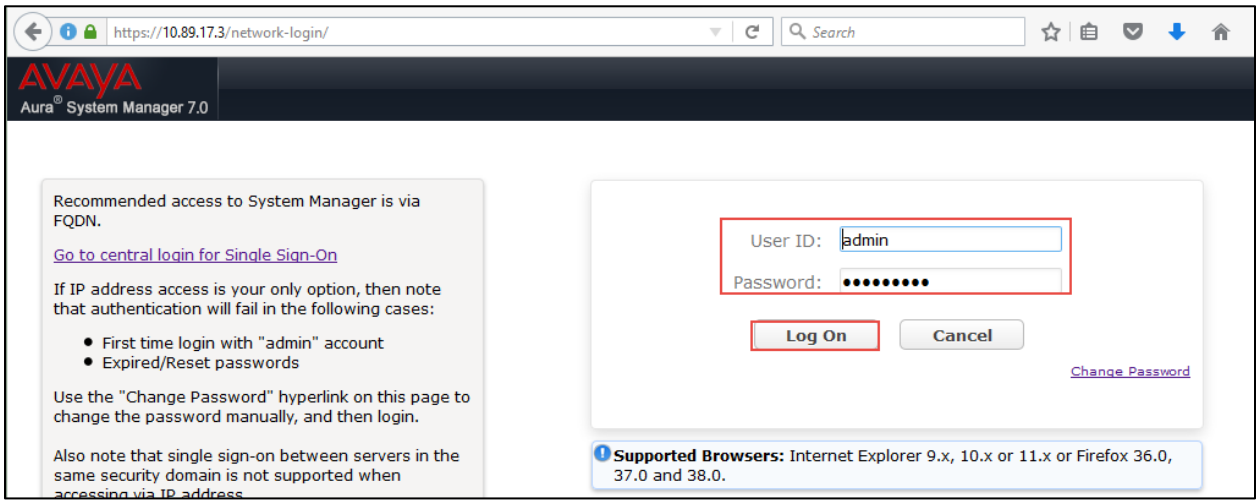


12. Configure **System:** *Lab126-CM7*, used in this example.
13. Configure **Profile Type**: *Endpoint*, used in this example.
14. Configure **Extension:** *2102*, used in this example.
15. Click **Done**.

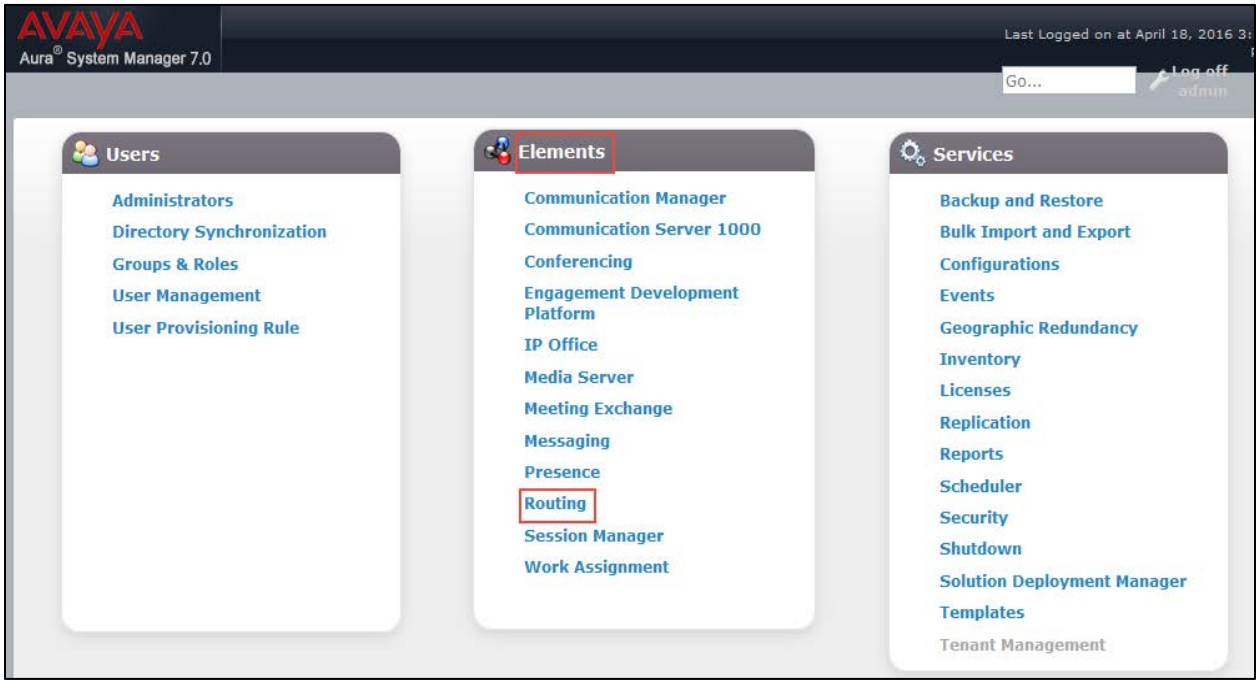
Avaya Aura Session Manger Configuration

1. Access the Avaya Aura System Manager Web login screen via **Error! Hyperlink reference not valid.** Address/FQDN>. IP address *10.89.17.3* is used in this example.
2. Log in with the User Id **admin** and associated password, and then click **Log On**.

Avaya Aura SM: Login Screen



Avaya Aura SM: Navigation Menu



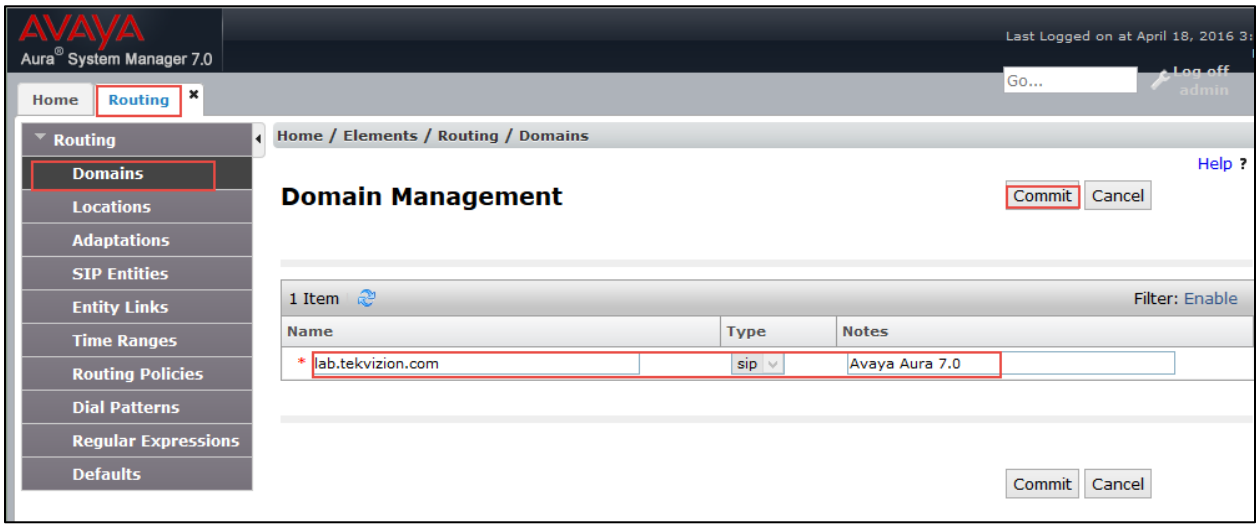
Domain

Create an SIP domain for each domain of which Session Manager will need to be aware of in order to route calls.

To configure a domain, perform the following procedure.

1. Navigate to **Home** > **Routing** > **Domains**.
2. Click **New**.
3. Enter the following information:
   - **Name:** Enter the domain name: *lab.tekvizion.com* was used in this example.
   - **Type:** Select **sip** from the pull-down menu.
   - **Notes:** Add a brief description (optional).
4. Click **Commit** to save.

Avaya Aura SM: Domain Configuration



Location

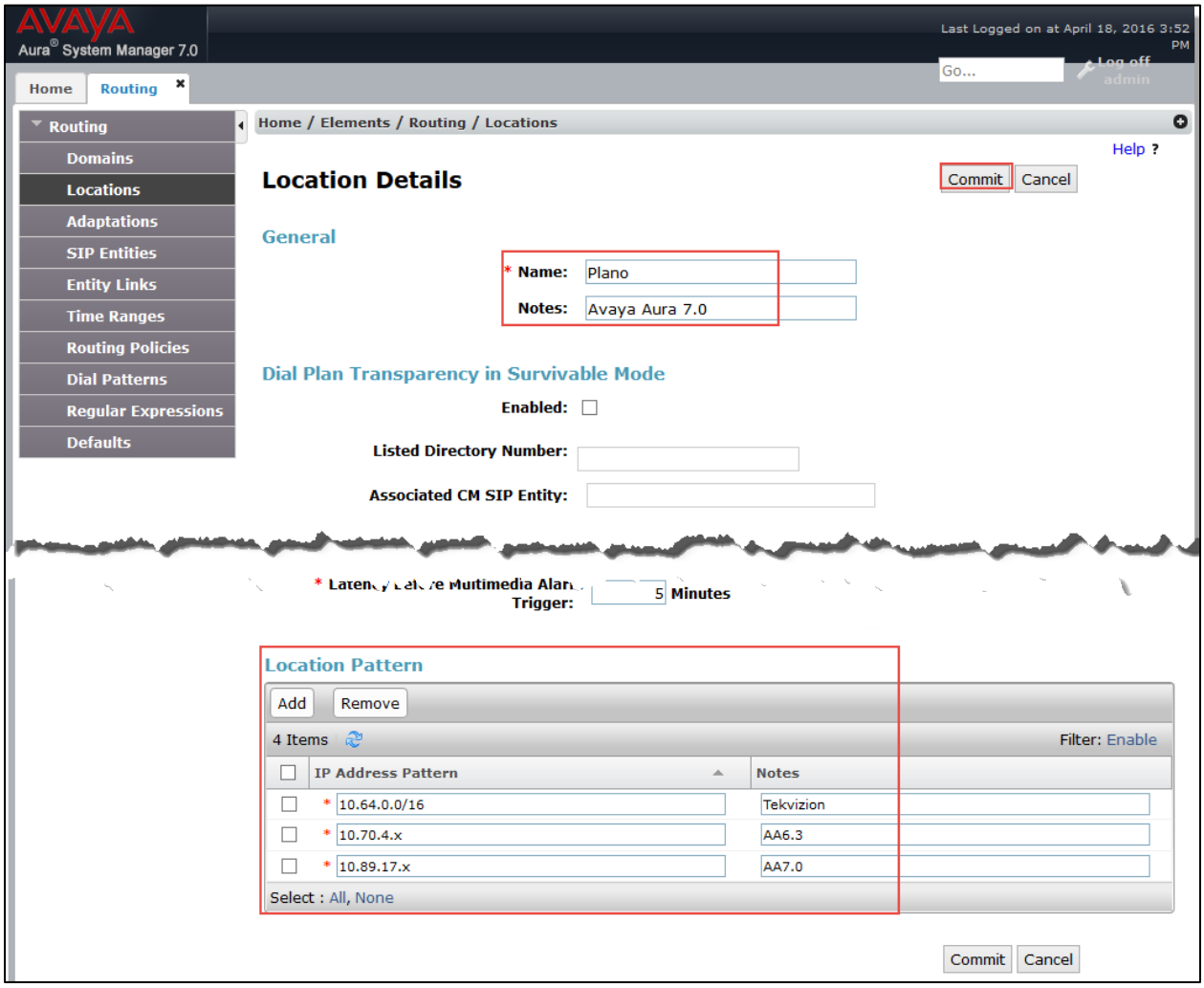
Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management and call admission control.

To add a location, perform the following procedure.

1. Navigate to **Routing** > **Locations**.
2. Click the **New** button.
3. In the **General** section, enter the following values:
   - **Name:** Enter a descriptive name for the location: *Plano* was used in this example.
   - **Notes:** Add a brief description (optional).
4. Retain all other default configurations..
5. Click **Commit** to save.

6. Under **Location Pattern**, click **Add** to add **IP Address Patterns** for different networks that are part of the topology:
    - **10.64.0.0/16**: tekVizion
    - **10.89.17.x**: AA7.0
7. Retain all other default configurations.
8. Click **Commit** to save.

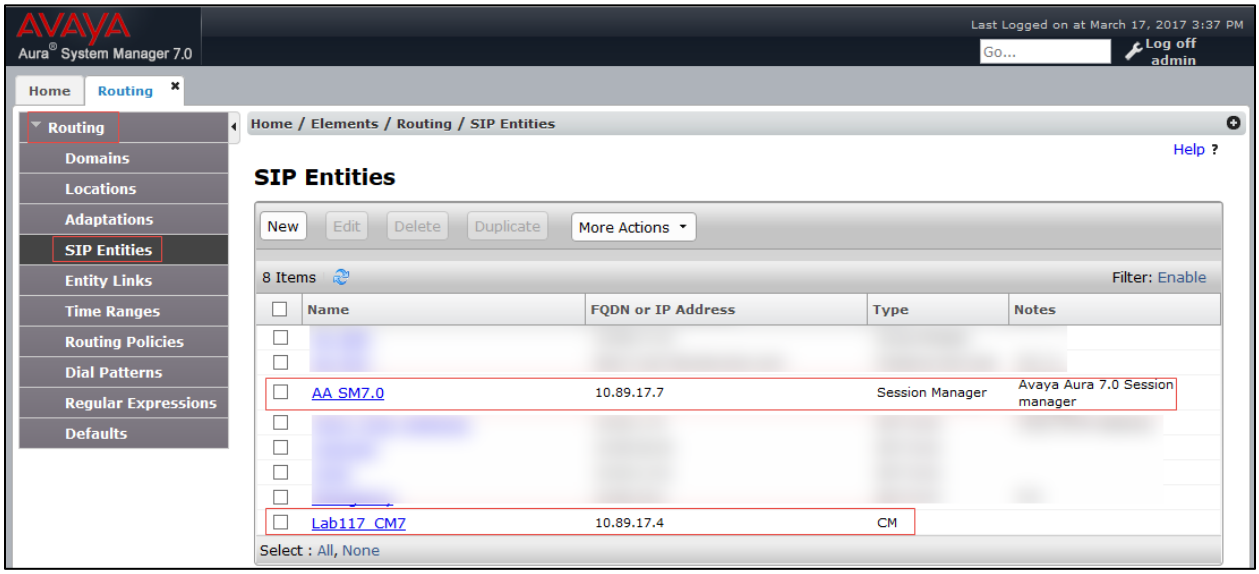
Avaya Aura SM: Location Configuration



SIP Entity and Entity links

A SIP entity must be added for each network element that is part of the topology and that will participate in the example. This includes the Session Manager, the Communication Manager, and the PSTN gateway.

Avaya Aura SM: SIP Entity

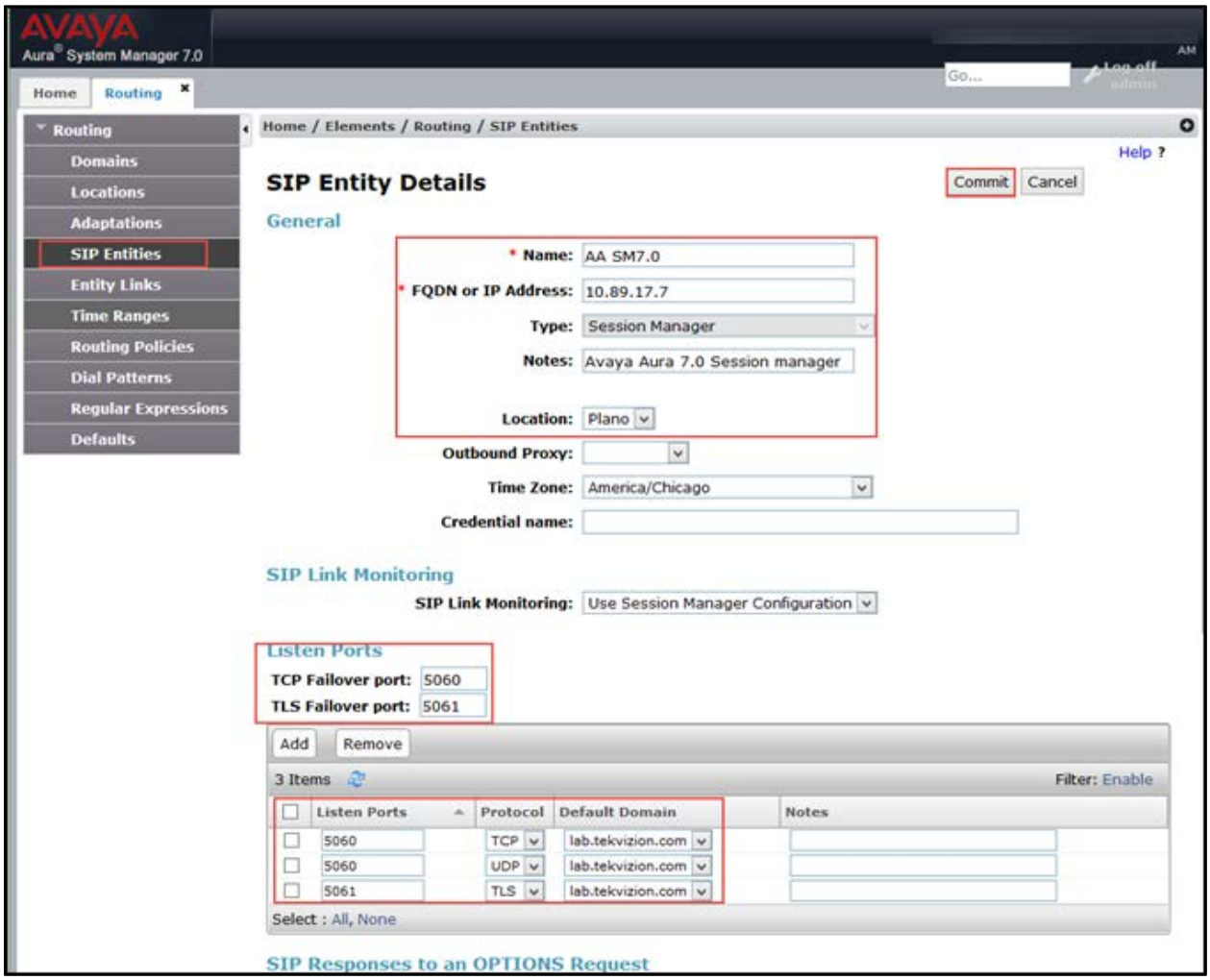


Add a SIP Entity for Session Manager

To add an SIP entity, perform the following procedure:

1. Navigate to **Routing** > **SIP Entities**.
2. Click on the **New** button.

Avaya Aura CM Configuration: SIP Entity (1/2)



3. In the General section, enter the following values:
   - **Name:** Enter a descriptive name. *AA SM7.0* was used for the Avaya SM in this example.
   - **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity interface that is used for SIP signaling: *10.89.17.7* was used in this example.
   - **Type:** Enter *Session Manager*.
   - **Location:** Select one of the locations defined previously: *Plano* was used in this example.
   - **Time Zone:** Select the time zone for the location entered above: *American/Chicago* was used in this example.

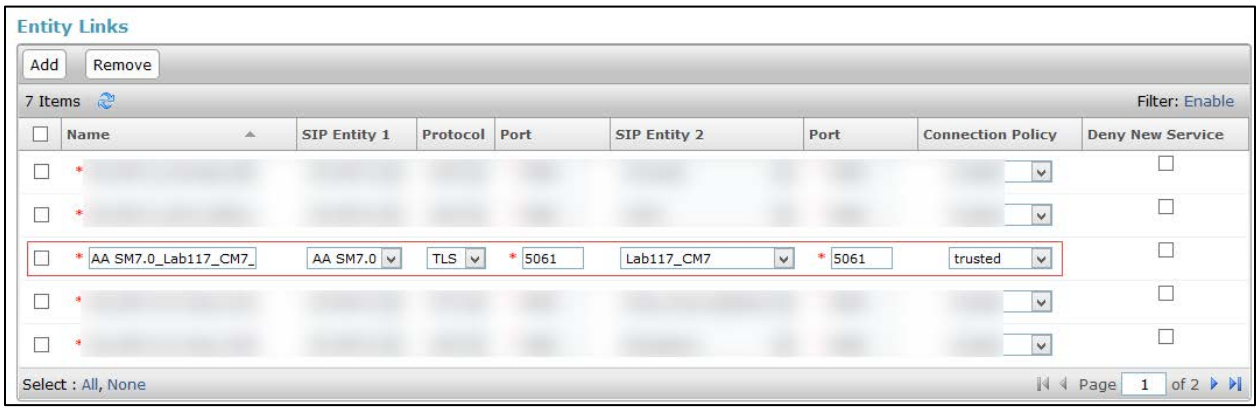
- To define the ports used by Session Manager, scroll down to the **Port** section.
- In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:
  - **Port:** Enter the port number on which the CM will listen for SIP requests: *5060* was used in this example.
  - **Protocol:** Transport protocol to be used to send SIP requests: *TCP* was used in this example.
  - Add another entry with **Port 5061** and **Protocol TLS** with the **Default domain** as **lab.tekvizion.com** configured earlier.

The SIP entity link for this entity is added after the CM entity has been configured.

To configure the SIP entity link for the SM, perform the following procedure.

1. Under **Entity Links**, Click **Add**.

Avaya Aura CM: SIP Entity-CM Configuration (2/2)

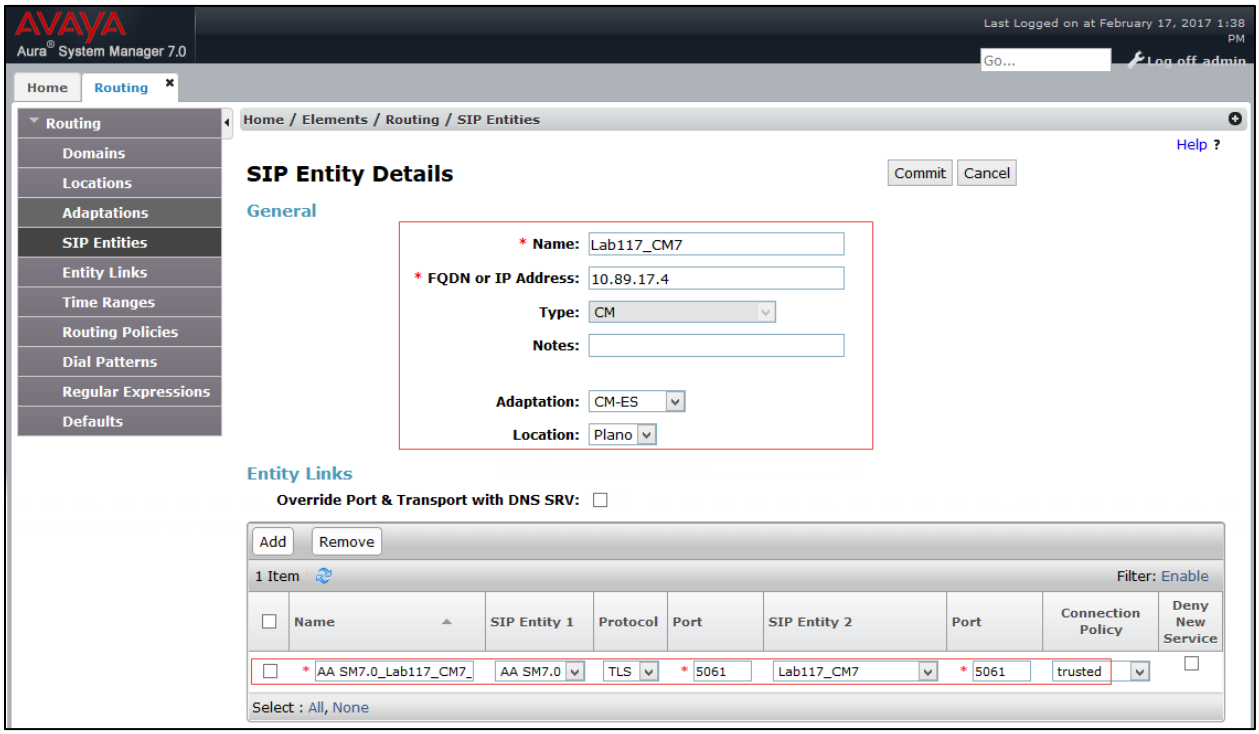


- Set **SIP Entity 1**: Select **AA SM7.0**, which is configured in the previous step from the drop-down menu.
- Set **SIP Entity 2**: Retain the default value: **Lab117_ CM7**
- Set **Protocol**: *tls* is used in this example.
- Set **Ports**: set both ports to **5061**.
- Set **Connection Policy**: **trusted**.

2. Retain all other default configurations..
3. Click **Commit**.

Add SIP Entity and Link for Communication Manager

Avaya Aura SM: SIP Entity and Entity Link CM Configuration



To add a SIP entity for the Avaya CM, follow this procedure:

1. Enter the following information.
   - Name: *Lab116-CM7* is used this example for an SIP entity of Avaya CM.
   - IP address: *10.89.17.4* is used in this example.
   - Type: *CM* is used in this example.
   - Notes: Add a description.
   - Adaptation: *CM-ES* is used in this example.
   - Location: Select one of the locations defined previously: *Plano* is used in this example.
   - Time Zone: Select the time zone for the location above.
2. Under Entity Links, Click Add.
   - Set SIP Entity 1: Select *AA SM7.0* which is configured in previous step from the drop-down menu.
   - Set SIP Entity 2: Retain the default value: *AA CM7*.
   - Set Protocol: TLS.
   - Set Ports: set both ports to 5061.
   - Set Connection Policy: trusted.
3. Retain all other default configurations..

4. Click **Commit**.

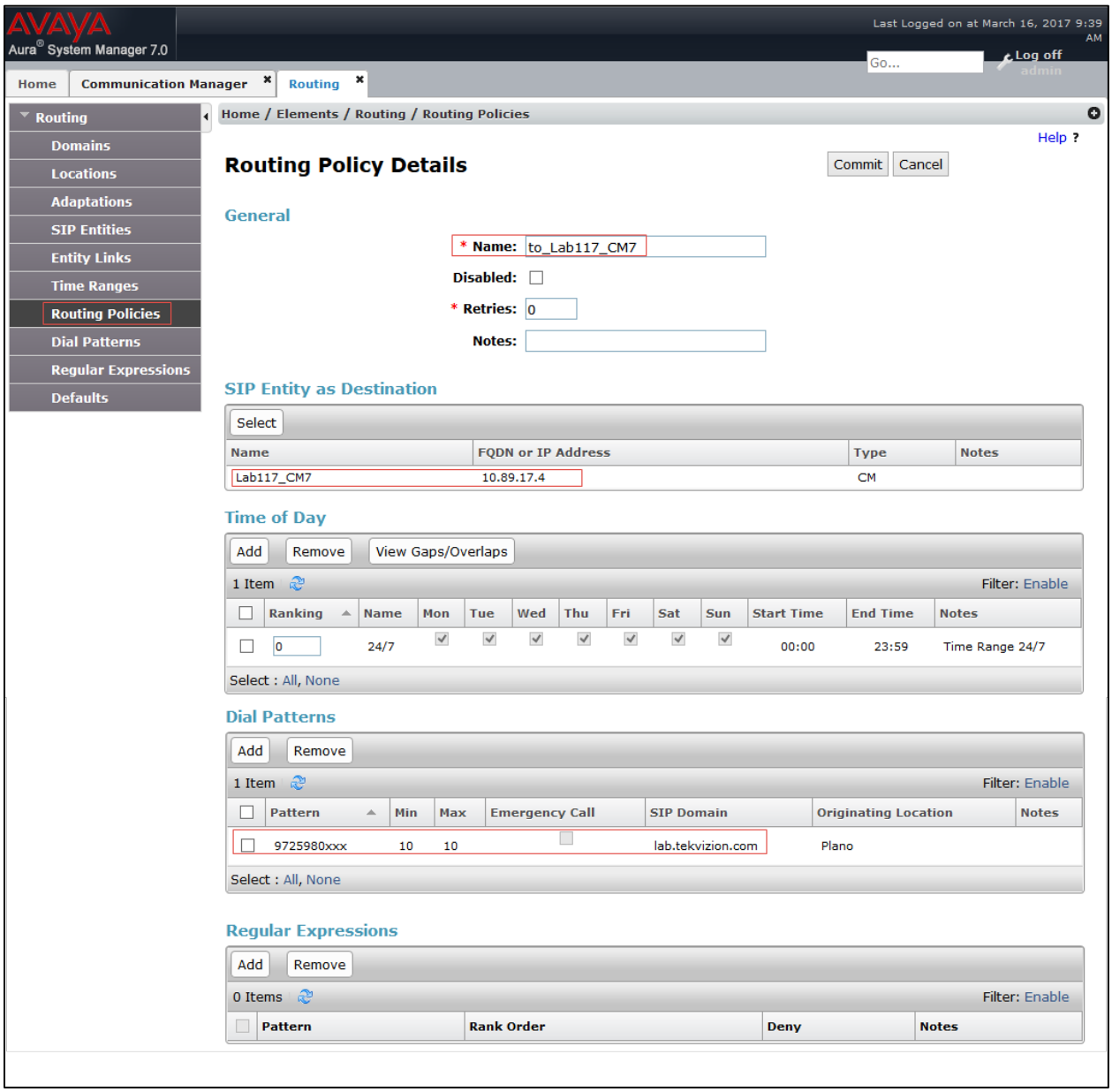
Routing Policy

Routing Policies describe the conditions under which calls are routed to the SIP entities. Three routing policies were added for this example: one for Communication Manager, one for voicemail, and one for the PSTN GW.

To add a routing policy for Avaya CM, perform the following procedure.

1. Navigate to **Routing** > **Routing Policies**.
2. Click on the **New** button.

Avaya Aura SM: Routing Policy Configuration



3. In the General section, enter the following values.
   - Name: *to_Lab117_CM7* is used in this example.
   - SIP Entity as Destination: Select the Avaya CM: *Lab117-CM7* is used in this example.
   - Retain all other default configurations.
4. Add the following Dial patterns that can be routed using this policy:
   - Pattern: 9725980xxx> 10 digit Avaya and Crestron endpoints DID starting with 9725980.

Security Configuration and Management

For this example, the Avaya Aura System Manager served as the Certificate Authority.

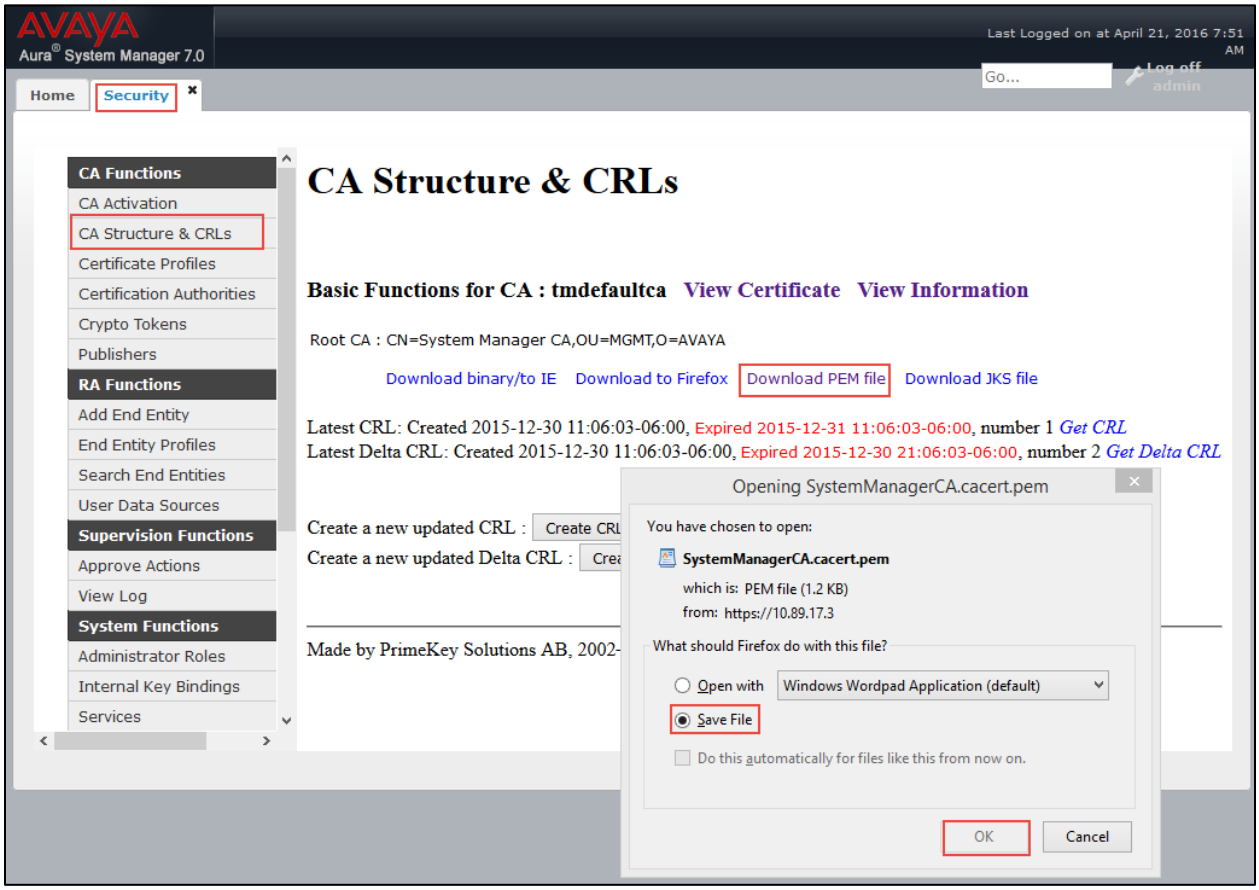
The system manager trusted root certificates must be installed on the Crestron Mercury device that communicates with Session Manager over TLS.

Exporting the System Manager CA

Follow this procedure to export the system manager CA:

1. Navigate to **Services** > **Security** > **Certificate** > **Authority** > **CA Structure & CRLs**.

Avaya Aura SM: Export System Manager CA



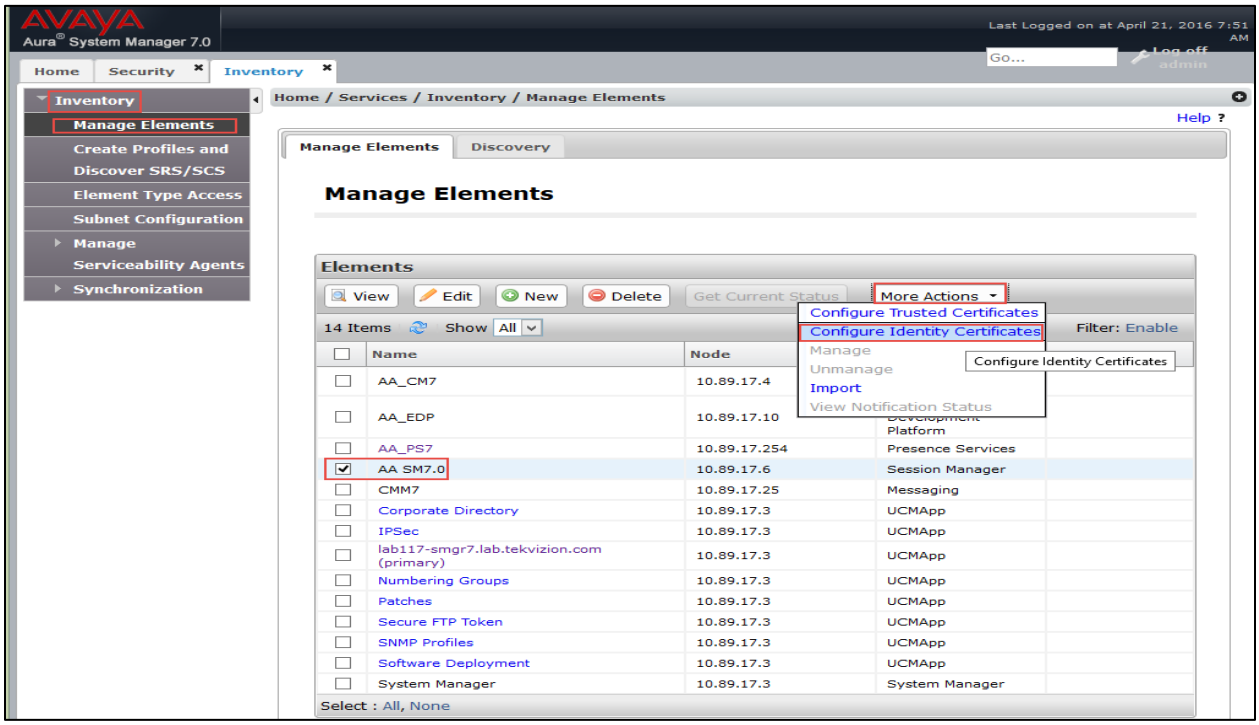
2. Click **Download PEM file**.
3. Select **Save File**.
4. Click **OK**.

Replace Session Manager Identity Certificate

To replace a session manager identity certificate, follow this procedure:

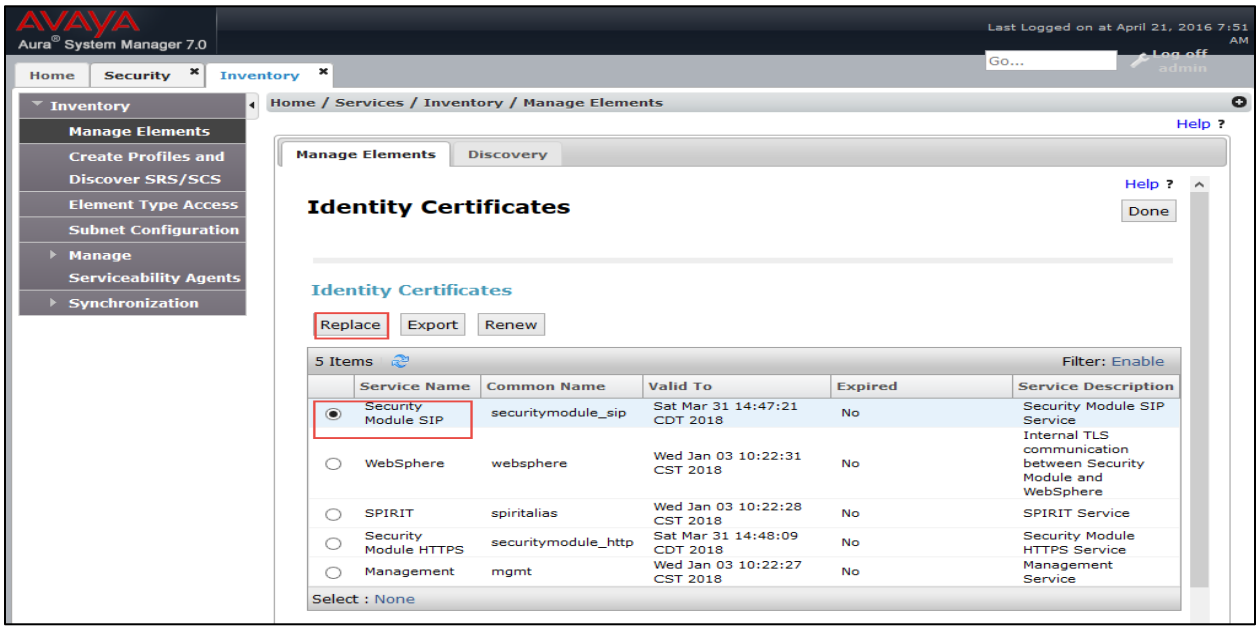
1. Navigate to Services > Inventory > Manage Element.

Configuring the Identity Certificate



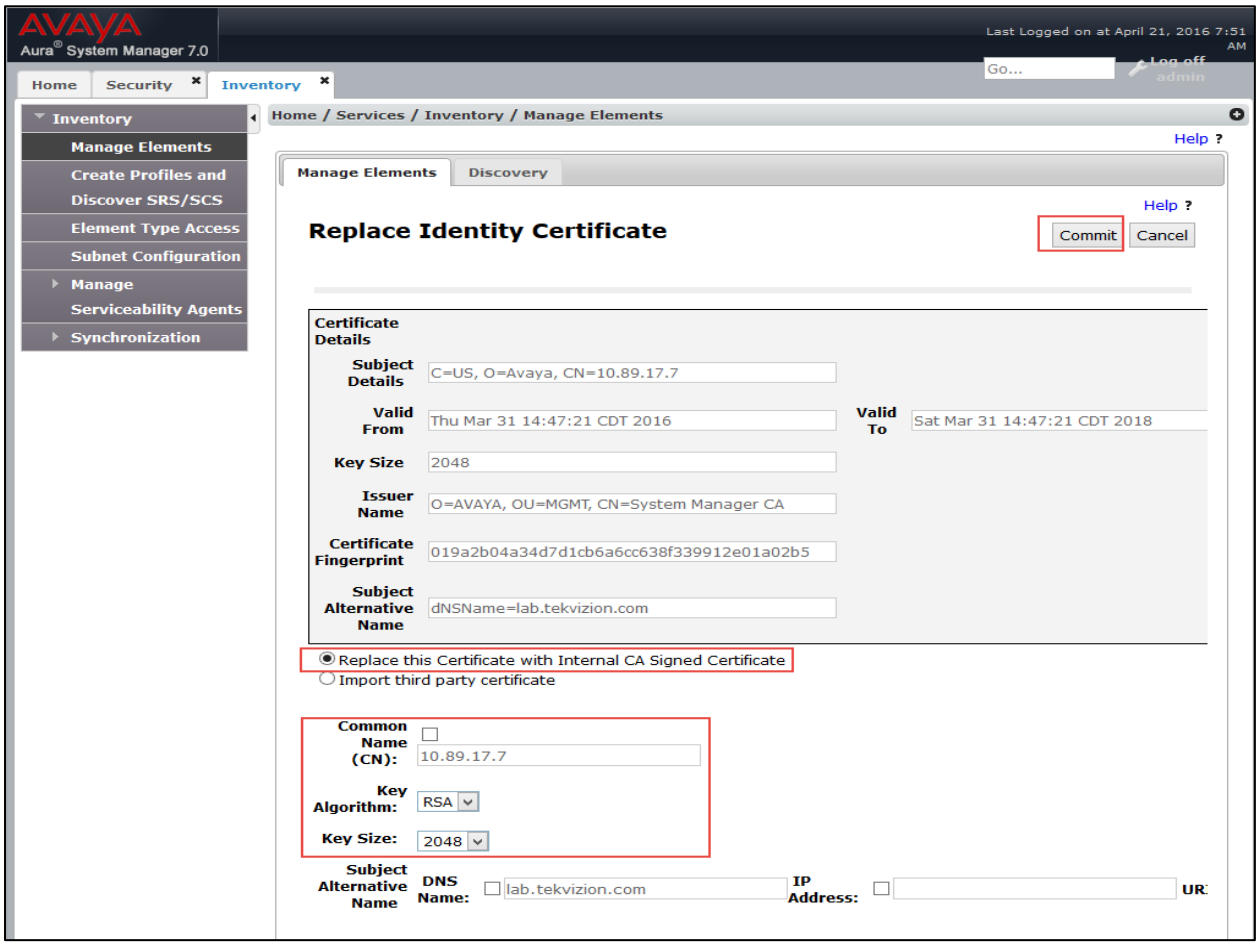
2. Select the proper session manager: *AA SM7.0* is selected for this setup.
3. Click More Actions.
4. Select Configure Identity Certificate.

Initiating a Replace of Identity Certificate



5. Select **Security Module SIP**.
6. Click **Replace**.

Replace identity Certificate



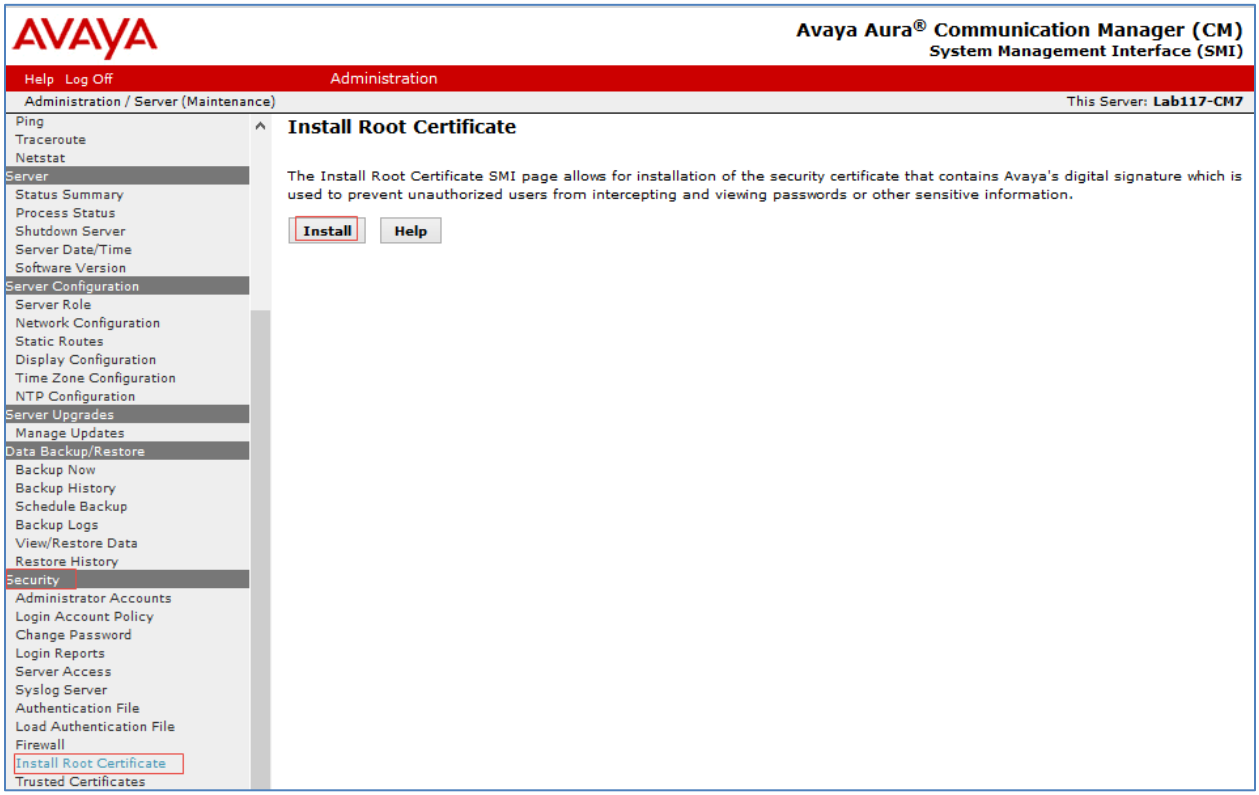
7. Select **Replace this Certificate with Internal CA signed Certificate**.
8. Set **Common Name**: The SIP IP address *10.89.17.7* is used in this setup.
9. Set **Key Algorithm**: *RSA* is selected from the drop-down menu.
10. Set **Key Size**: *2048* is selected for the setup.
11. Click **Commit**.
12. Repeat for **Security Module HTTPS**.

Upload Root Certificate to Avaya CM

To upload a root certificate to Avaya CM, follow this procedure:

1. On the Communication Manager Administration web UI, navigate to Security > Install Root Certificate.
2. Click Install.

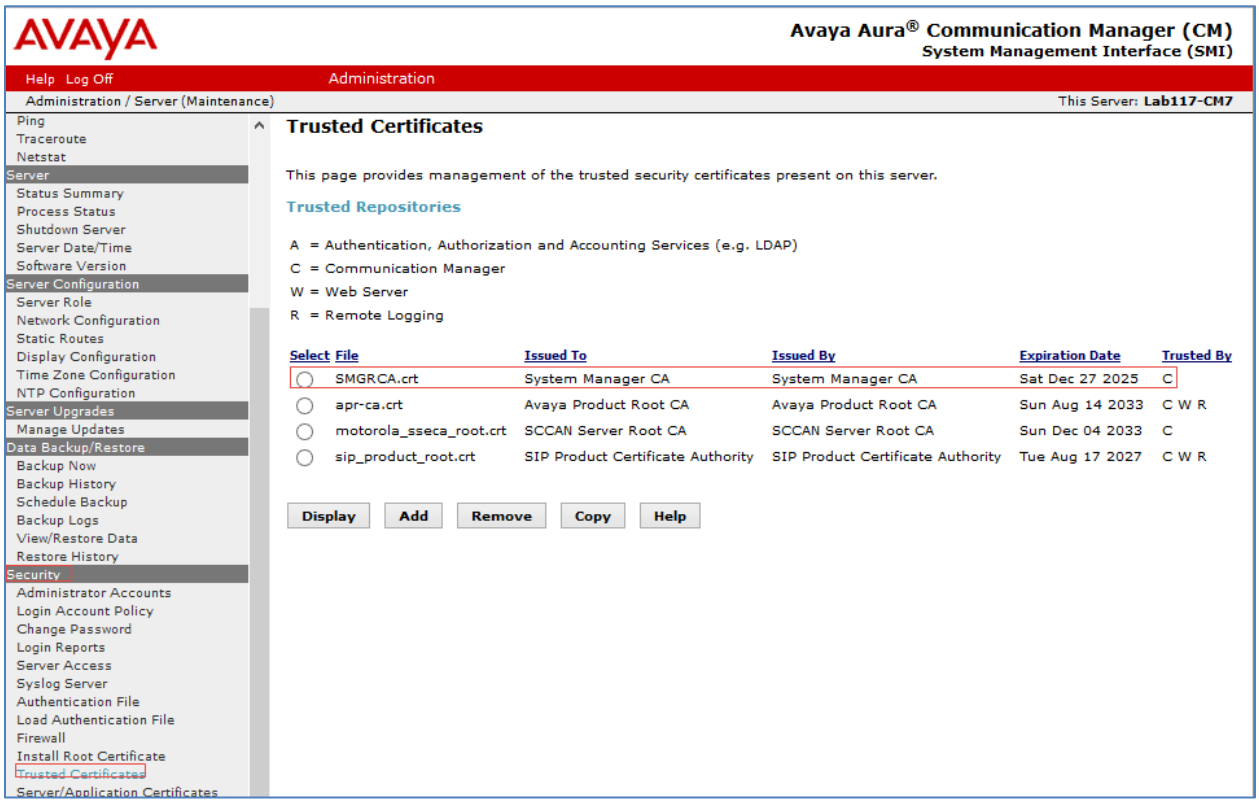
Avaya CM: Install Root Certificate



3. Click OK on the screen that follows (not shown).

Once the certificate is installed, verify that it is listed under the Trusted Certificates (navigate to: Security > Trusted Certificates). The root certificate installed above should be listed under the trusted certificates (as *SMGRCA.crt*).

Avaya CM: Trusted Certificates



Avaya 46xx File settings

The 46xx file settings that were configured for the example are shown below.

- SIP_CONTROLLER_LIST: *10.89.17.7:5061;transport=tls* was configured for secure SIP example.ing.
- ENFORCE_SIPS_URI: *0-No*. This disabled the system from requiring sip messages to be in the sips format.
- TRUSTCERTS: Specific trust certificates that need to be downloaded to the Avaya phones for them to function in a secure mode. This includes a certificate from the rootCA, in addition to the default certificates that exist on the phone.
- ENABLE_G729: *1-Enable G729A* was used in this example for G729 support on Crestron Mercury.
- MEDIAENCRYPTION: *1*, i.e., Enabled.

Avaya Aura: 46xx File Settings

Activate	Parameter	Value
☑	SIPDOMAIN	lab.tekvizion.com
☑	SIP_CONTROLLER_LIST	10.89.17.7:5061;transport=tls,
☑	SIPPROXYSRVR	10.89.17.7
☑	MWISRVR	10.89.17.25
☑	SNTPSRVR	10.10.10.5
☑	TIMEZONE	American/Chicago
☑	ENABLE_PRESENCE	1 - Display and signal presence information.
☑	PRESENCE_SERVER	10.89.17.15
☑	ENABLE_AUTOMATIC_ON_THE_PHONE_PRESENCE	1 - Send on/off hook updates.
☑	MUTE_ON_REMOTE_OFF_HOOK	0
☑	ENFORCE_SIPS_URI	0 - No
☑	100REL_SUPPORT	1
☑	DISPLAY_NAME_NUMBER	1 - Show caller name and number
☑	TRUSTCERTS	Lab117_rootca.txt,av_prca_pem_2033.txt,av_sipca_pem_2027.tx
☑	TLSSRVRID	0 - No certificate match is necessary.
☑	ENABLE_G711A	0 - Disable G711A
☑	ENABLE_G711U	1 - Enable G711U
☑	ENABLE_G729	1 - Enable G729A
☑	SEND_DTMF_TYPE	2 - Use RFC 2833 out-of-band DTMF
☑	DTMF_PAYLOAD_TYPE	96

This page is intentionally left blank.

Crestron Electronics, Inc.
15 Volvo Drive Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7576
www.crestron.com

Configuration Guide – DOC. 7990A
(2048829)
05.17
Specifications subject to
change without notice.