



Avaya Solution & Interoperability Test Lab

Application Notes for Polycom Trio™ Conference Phones and Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Polycom Trio™ Conference Phones which were compliance tested with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

The overall objective of the interoperability compliance testing is to verify Polycom Trio™ Conference Phone functionalities in an environment comprised of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and various Avaya 9600 Series IP Deskphones.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures for configuring Polycom Trio™ Conference Phones (Trio) which were compliance tested with Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Session Manager (Session Manager). Trio registers via SIP/TLS for signaling and SRTP for audio.

Two models of Trio were tested during compliance testing; Trio 8800 and Trio 8500. Trio registers with Session Manager as SIP endpoints combining the functionality of IP phone and conferencing station in support of voice communications and conferencing requirements. Trio 8800 and Trio 8500 use the same SIP software stack and provisioning model.

These Application Notes assume that Communication Manager and Session Manager are already installed, and basic configuration steps have been performed. Only steps relevant to this compliance test will be described in this document. For further details on configuration steps not covered in this document, consult references [1], [2] and [3].

2. General Test Approach and Test Results

The general test approach was to place calls to and from Trio and exercise basic telephone operations. The main objectives were to verify the following:

- Registration
- Caller ID display
- Codecs (G.711MU, G.711A, G.722-64 and G.729)
- Media Shuffling enabled and disabled
- Inbound calls
- Outbound calls
- Hold/Resume
- Call termination (origination/destination)
- Conferences and Transfers (origination/destination)
- Use of Avaya Feature Access Codes (FACs)
- Long duration calls to verify Session Timers
- MWI
- Voicemail
- Serviceability

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect

Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Polycom Trio utilized enabled capabilities of secure connectivity via TLS/SRTP.

2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of interoperability compliance testing was primarily on verifying call establishment on Trio. Trio operations such as inbound calls, outbound calls, hold/resume, transfer, conference, FACs, and Trio interactions with Session Manager, and Avaya SIP and H.323 telephones were verified. The serviceability testing introduced failure scenarios to see if Trio 8800 and Trio 8500 can recover from failures.

2.2. Test Results

The test objectives were verified. For serviceability testing, Trio operated properly after recovering from failures such as cable disconnects, and resets of Trio and Session Manager. The features tested worked as expected.

2.3. Support

For technical support on Polycom Trio Conference Phones, please contact via the following:

Web: <http://support.polycom.com>

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya Aura® environment and, Trio 8800 and Trio 8500.

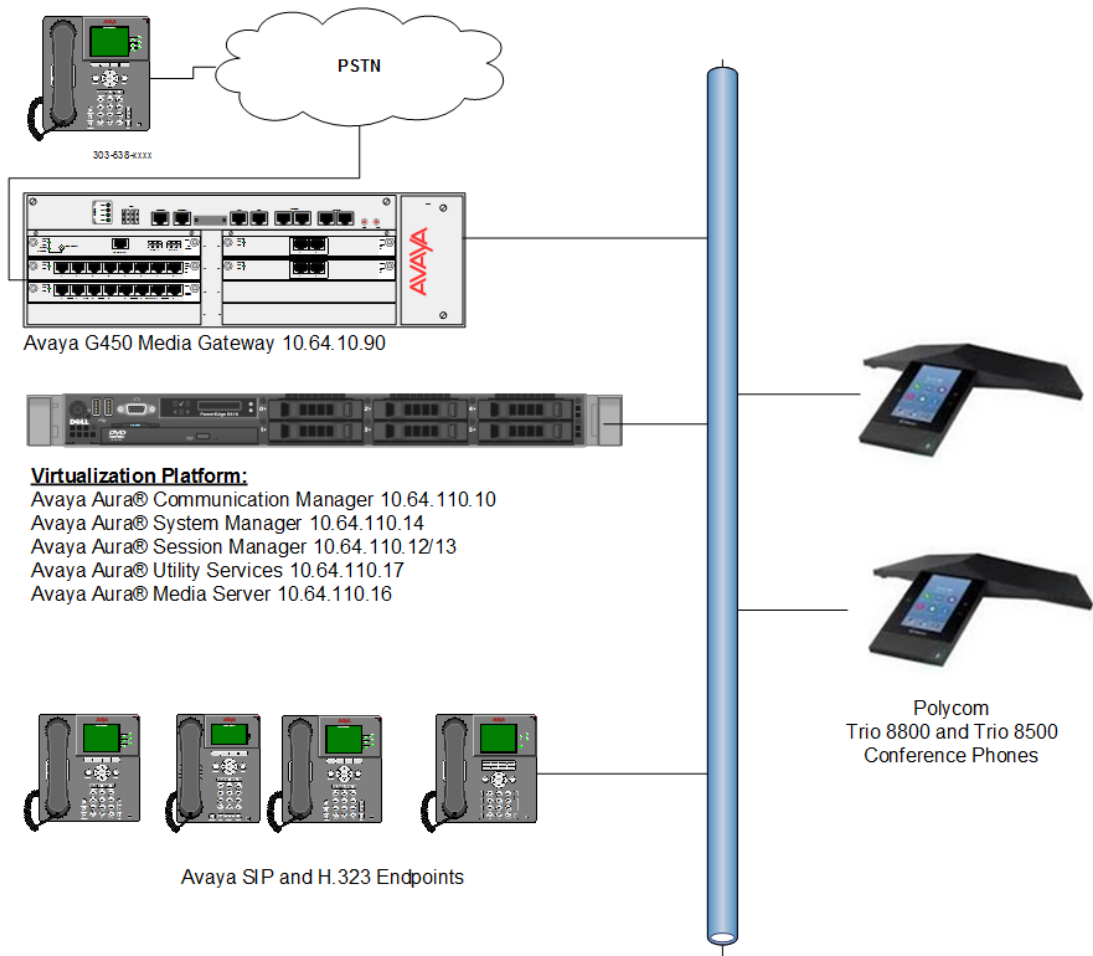


Figure 1: Test Configuration of Polycom Trio

4. Equipment and Software Validated

The following equipment and software were used for the test configuration.

Equipment	Software/Firmware
Avaya Aura® Session Manager	8.0.0.0.800035
Avaya Aura® System Manager	8.0.0.0.931077
Avaya Aura® Communication Manager	8.0.0.1.2 Service Pack 1 Patch 2
Avaya G450 Media Gateway	40.10.1
Avaya 9600 Series IP Deskphones	
SIP 96x0	2.6.17
SIP 96x1	7.1.3.0
H.323 96x0	3.2.8
H.323 96x1	6.7.0
Polycom Trio™ conference phones	5.7.2.3205

5. Configure the Avaya Aura® Communication Manager

This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, and a SIP station. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface.

In this section, the following topics are discussed:

- Capacity Verification
- IP Codec Set
- IP Network Region
- IP Node Name
- Signaling Group
- Trunk Group

5.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient **Maximum Off-PBX Telephones – OPS** licenses. If not, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options                               Page 1 of 12
                                OPTIONAL FEATURES

G3 Version: ?                               Software Package: Enterprise
Location: 2                                 System ID (SID): 1
Platform: 28                               Module ID (MID): 1

                                USED
                                Platform Maximum Ports: 48000 23
                                Maximum Stations: 36000 8
                                Maximum XMOBILE Stations: 36000 0
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 2
Maximum Off-PBX Telephones - PBFMC: 41000 0
Maximum Off-PBX Telephones - PVFMC: 41000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
                                Maximum Survivable Processors: 313 0
```

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options           Page 2 of 12
                OPTIONAL FEATURES

IP PORT CAPACITIES                                USED
      Maximum Administered H.323 Trunks: 12000 0
Maximum Concurrently Registered IP Stations: 2400 5
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 2400 0
      Maximum Concurrently Registered IP eCons: 128 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 36000 0
      Maximum Video Capable IP Softphones: 2400 0
      Maximum Administered SIP Trunks: 12000 10
Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 688 0
```

5.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.3** for configuring IP network region to specify which codec sets may be used within and between network regions. For the compliance testing, G.711MU, G.711A, G.722-64K and G.729 were tested for verification. Also, configure the SRTP profiles as show under **Media Encryption** section.

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

                                IP MEDIA PARAMETERS

Codec Set: 1

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: G.722-64K   2           2        20
5:
6:
7:

Media Encryption                               Encrypted SRTCP: enforce-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3: 3-srtp-aescm128-hmac80-unauth
4: 4-srtp-aescm128-hmac32-unauth
5:
```


5.3. Configure IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and Session Manager. Enter the **change ip-network-region <n>** command, where **n** is a number between **1** and **250** inclusive, and configure the following:

- **Authoritative Domain** – Enter the appropriate name for the Authoritative Domain. Set to the appropriate domain. During the compliance test, the authoritative domain is set to **avaya.com**. This should match the SIP Domain value on Session Manager, in **Section 6.1**.
- **Intra-region IP-IP Direct Audio** – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in the same IP network region. The default value for this field is **yes**.
- **Codec Set** – Set the codec set number as provisioned in **Section 5.2**.
- **Inter-region IP-IP Direct Audio** – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in different IP network regions. The default value for this field is **yes**.

```
change ip-network-region 1                                     Page 1 of 20
                                                              IP NETWORK REGION
Region: 1
Location: 1          Authoritative Domain: avaya.com
Name: Default       Stub Network Region: n
MEDIA PARAMETERS    Intra-region IP-IP Direct Audio: yes
                   Codec Set: 1                Inter-region IP-IP Direct Audio: yes
                   UDP Port Min: 2048           IP Audio Hairpinning? y
                   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 44
Audio PHB Value: 44
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
```

5.4. Configure IP Node Name

This section describes the steps for setting IP node name for Session Manager in Communication Manager. Enter the **change node-names ip** command, and add a node name for Session Manager along with its SIP Entity IP address from **Section 6.3**.

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
  Name          IP Address
  aes8          10.64.110.132
  ams8          10.64.110.136
  default       0.0.0.0
  procr        10.64.110.131
  procr6       ::
  sm8         10.64.110.135

( 6 of 6 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
```

5.5. Configure Signaling Group

This section describes the steps for administering a signaling group in Communication Manager for communication between Communication Manager and Session Manager. Enter the **add signaling-group <s>** command, where s is an available signaling group and configure the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- **Near-end Node Name** – Set to **procr**.
- **Far-end Node Name** – Set to the Session Manager name configured in **Section 5.4**.
- **Far-end Network Region** – Set to the region configured in **Section 5.3**.
- **Far-end Domain** – Set to **avaya.com**. This should match the SIP Domain value in **Section 6.1**.
- **Direct IP-IP Audio Connections** – Set to **y**, since Media Shuffling is enabled during the compliance test.

Note that **Enforce SIPS URI for SRTP** was not enabled because Trio does not use SIPS URIs when generating a call. It does, however, accept and processes SIPS URIs for a call it receives.

```
add 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? 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: sm8
  Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                           Far-end Network Region: 1

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate                Bypass If IP Threshold Exceeded? n
  DTMF over IP: rtp-payload                RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3                Direct IP-IP Audio Connections? y
  Enable Layer 3 Test? y                IP Audio Hairpinning? y
H.323 Station Outgoing Direct Media? n                Initial IP-IP Direct Media? n
                                           Alternate Route Timer(sec): 6
```

5.6. Configure Trunk Group

This section describes the steps for administering a trunk group in Communication Manager for communication between Communication Manager and Session Manager. Enter the **add trunk-group** <t> command, where **t** is an unallocated trunk group and configure the following:

- **Group Type** – Set the Group Type field to **sip**.
- **Group Name** – Enter a descriptive name.
- **TAC** (Trunk Access Code) – Set to any available trunk access code.
- **Service Type** – Set to **tie**.
- **Signaling Group** – Set to the Group Number field value configured in **Section 5.5**.
- **Number of Members** – Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
change trunk-group 1                                     Page 1 of 5
                                     TRUNK GROUP
Group Number: 1                Group Type: sip          CDR Reports: y
  Group Name: sm8                COR: 1              TN: 1          TAC: 101
  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
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: Session Manager server and System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager for call processing.

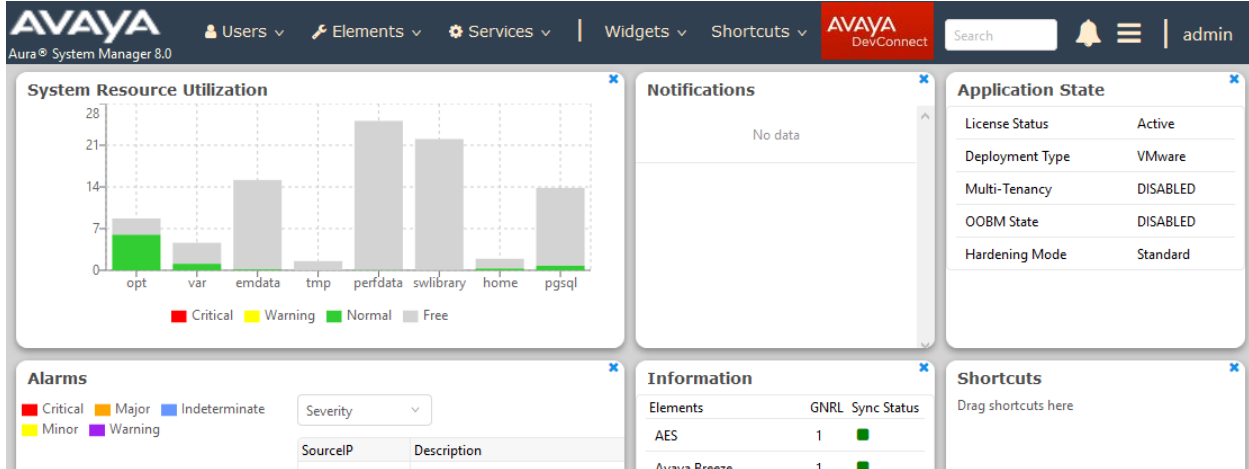
In this section, the following topics are discussed:

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- User Management

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

6.1. Configure SIP Domain

Launch a web browser, enter <http://<IP address of System Manager>> in the URL, and log in with the appropriate credentials.

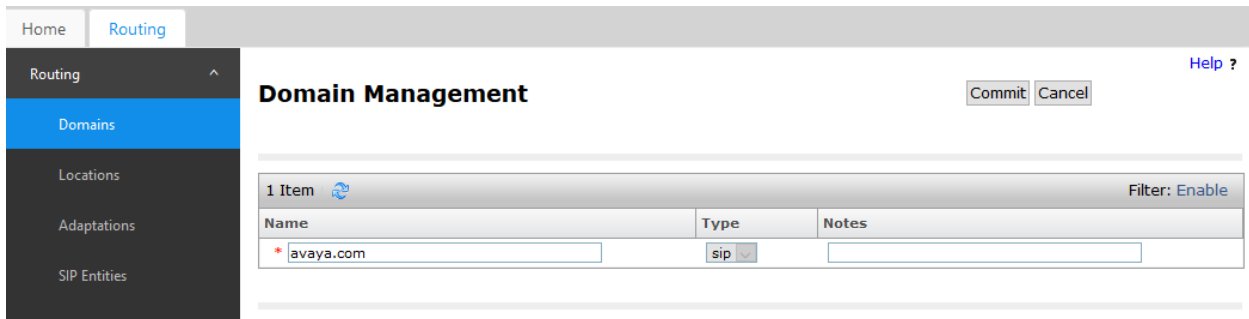


In the main menu, navigate to **Elements** → **Routing** → **Domains**, and click on the **New** button (not shown) to create a new SIP Domain. Enter the following values and use default values for remaining fields:

- **Name** – Enter the Authoritative Domain Name specified in **Section 5.3**, which is **avaya.com**.
- **Type** – Select **SIP**

Click **Commit** to save.

The following screen displays the Domains page used during the compliance test.



6.2. Configure Locations

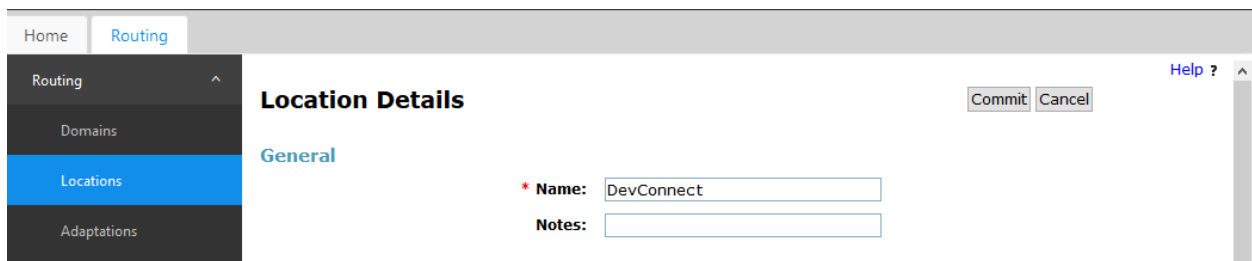
Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

From the main menu, navigate to **Elements** → **Routing** → **Locations**, and click on the **New** button (not shown) to create a new SIP endpoint location.

General section

Enter the following values and use default values for remaining fields.

- Enter a descriptive Location name in the **Name** field (e.g. **DevConnect**).
- Enter a description in the **Notes** field if desired.



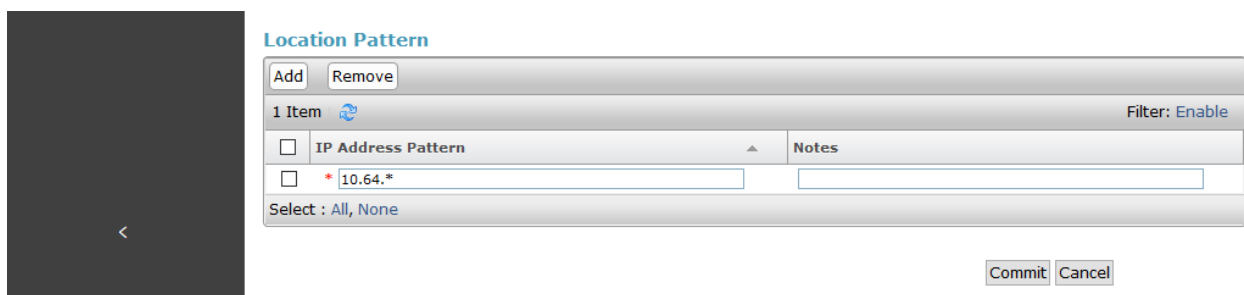
The screenshot shows the 'Location Details' form in the 'Routing' section. The 'General' section is active, showing a 'Name' field with the value 'DevConnect' and an empty 'Notes' field. There are 'Commit' and 'Cancel' buttons at the top right. A sidebar on the left shows 'Routing' selected, with 'Domains', 'Locations', and 'Adaptations' below it.

Location Pattern section

Click **Add** and enter the following values:

- Enter the IP address information for the **IP address Pattern** field (e.g. **10.64.***).
- Enter a description in the **Notes** field if desired.

Repeat steps in the Location Pattern section if the Location has multiple IP segments. Modify the remaining values on the form, if necessary; otherwise, use all the default values. Click on the **Commit** button.



The screenshot shows the 'Location Pattern' section. It features an 'Add' button and a 'Remove' button. Below, there is a table with one item. The table has columns for 'IP Address Pattern' and 'Notes'. The 'IP Address Pattern' field contains '*10.64.*' and the 'Notes' field is empty. There is a 'Filter: Enable' button and a 'Select : All, None' dropdown. 'Commit' and 'Cancel' buttons are at the bottom right.

6.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. During the compliance test, the following SIP Entities were configured:

- Session Manager: This entity was created prior to the compliance test.
- Communication Manager : This entity was created prior to the compliance test.
- Communication Manager Messaging : This entity was created prior to the compliance test.

Navigate to **Routing** → **SIP Entities** and click on the **New** button (not shown) to create a new SIP entity. Provide the following information:

General section

Enter the following values and use default values for remaining fields.

- Enter a descriptive Entity name in the **Name** field.
- Enter IP address for signaling interface on each Communication Manager, Session Manager, or Messaging in the **FQDN or IP Address** field
- From the **Type** drop down menu select a type that best matches the SIP Entity.
 - For Communication Manager, select CM
 - For Session Manager, select Session Manager
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

SIP Link Monitoring section

- Accept the other default values.

Click on the **Commit** button to save each SIP entity.

The following screen shows the SIP Entities page used during the compliance test. Note that the sm8 SIP Entity IP Address was used in **Section 5.4** for Session Manager.

The screenshot shows the 'SIP Entities' page in a web interface. The page has a navigation menu on the left with 'SIP Entities' selected. The main content area shows a table with 7 items. The items are:

Name	FQDN or IP Address	Type	Notes
aaep	10.64.110.50	Voice Portal	
asbce	10.64.110.32	SIP Trunk	
brz8	10.64.110.138	Avaya Breeze	
cm8	10.64.110.131	CM	
cmm8	10.64.110.133	Messaging	
ps8	ps8.avaya.com	Presence Services	
sm8	10.64.110.135	Session Manager	

6.4. Configure Entity Links

Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ↔ Communication Manager: This entity link was created prior to the compliance test.
- Session Manager ↔ Communication Manager Messaging: This entity link was created prior to the compliance test.

Navigate to **Routing** → **Entity Links** and click on the **New** button (not shown) to create a new entity link. Provide the following information:

- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity shown in **Section 6.3** (e.g. **sm8**).
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
 - TLS – 5061
 - UDP or TCP – 5060
- In the **SIP Entity 2** drop down menu, select Communication Manager SIP entity or Communication Manager Messaging SIP entity.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Enter a description in the **Notes** field if desired.
- Accept the other default values.

Click on the **Commit** button to save each Entity Link definition.

The following screen shows the Entities Links page used during the compliance test.

Entity Links

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	sm8_aaep_5060_TCP	sm8	TCP	5060	aaep	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	sm8_asbce_5060_TCP	sm8	TCP	5060	asbce	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	sm8_brz8_5061_TLS	sm8	TLS	5061	brz8	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	sm8_cm8_5061_TLS	sm8	TLS	5061	cm8	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	sm8_cmm8_5061_TLS	sm8	TLS	5061	cmm8	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	sm8_ps8_5061_TLS	sm8	TLS	5062	ps8	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

Select : All, None

6.5. Time Ranges

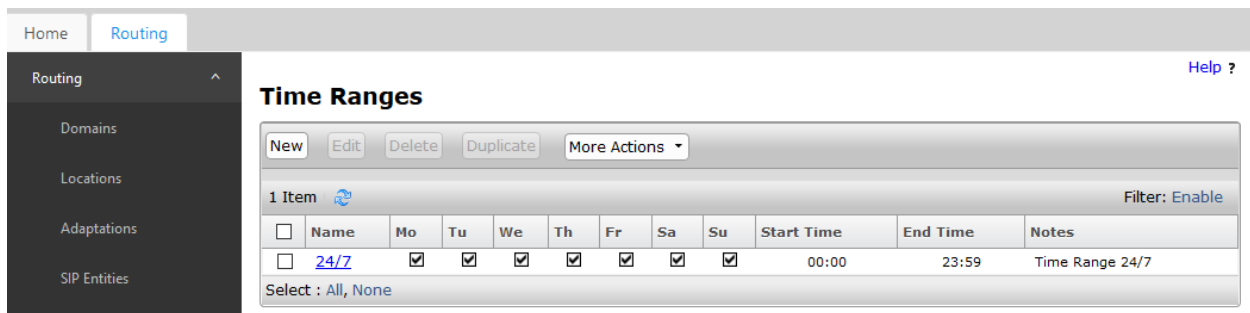
The Time Ranges form allows admission control criteria to be specified for Routing Policies (Section 6.6). In the reference configuration, no restrictions were used.

To add a Time Range, navigate to **Routing** → **Time Ranges**, and click on the **New** button (not shown). Provide the following information:

- Enter a descriptive Time Range name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

Click the **Commit** button.

The following screen shows the Time Range page used during the compliance test.



The screenshot shows a web interface for configuring Time Ranges. The top navigation bar includes 'Home' and 'Routing'. A sidebar on the left lists 'Routing' (expanded), 'Domains', 'Locations', 'Adaptations', and 'SIP Entities'. The main content area is titled 'Time Ranges' and features a 'Help ?' link. Below the title is a toolbar with buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table below the toolbar shows one item with the following details:

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

At the bottom of the table, there is a 'Select : All, None' option. The table also indicates '1 Item' and a 'Filter: Enable' option.

6.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 6.3**) with Time of Day admission control parameters (**Section 6.5**) and Dial Patterns (**Section 6.7**). In the reference configuration, Routing Policies are defined for:

- Calls to/from Communication Manager.
- Call to Communication Manager Messaging.

To add a Routing Policy, navigate to **Routing → Routing Policy**, and click on the **New** button (not shown) on the right. Provide the following information:

General section

- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.

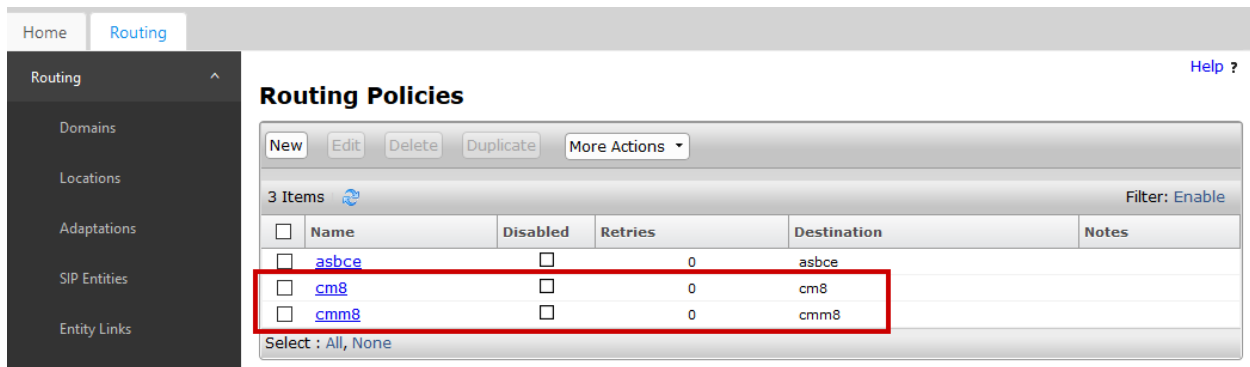
SIP Entity as Destination section

- Click the **Select** button.
- Select the SIP Entity that will be the destination for this call (not shown).
- Click the **Select** button and return to the Routing Policy Details form.

Time of Day section – Leave default values.

Click **Commit** to save Routing Policy definition.

The following screen shows the Routing Policies configured during compliance test.



The screenshot displays the 'Routing Policies' configuration page. On the left is a navigation menu with 'Routing' selected. The main content area shows a table of 3 items. The table has columns for Name, Disabled, Retries, Destination, and Notes. The rows are asbce, cm8, and cmm8. The cm8 and cmm8 rows are highlighted with a red box. Below the table is a 'Select : All, None' dropdown.

<input type="checkbox"/>	Name	Disabled	Retries	Destination	Notes
<input type="checkbox"/>	asbce	<input type="checkbox"/>	0	asbce	
<input type="checkbox"/>	cm8	<input type="checkbox"/>	0	cm8	
<input type="checkbox"/>	cmm8	<input type="checkbox"/>	0	cmm8	

6.7. Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the domain in the request URI is also examined. In the compliance test, the following dial patterns are defined from Session Manager.

- 5xxxx – SIP and H.323 endpoints on Communication Manager and Session Manager
- 59998 – Voicemail pilot number of Communication Manager Messaging.

To add a Dial Pattern, select **Routing → Dial Patterns**, and click on the **New** button (not shown) on the right. During the compliance test, 5-digit dial plan was utilized. Provide the following information:

General section

- Enter a unique pattern in the **Pattern** field (e.g. **5**).
- In the **Min** field enter the minimum number of digits (e.g. **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI received by Session Manager from Communication Manager.
- Enter a description in the **Notes** field if desired.

Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the boxes for the appropriate Originating Locations, and Routing Policies (see **Section 6.6**) that pertain to this Dial Pattern.
 - Originating Location – Check the **Apply The Selected Routing Policies to All Originating Locations** box.
 - Routing Policies for Communication Manager or Communication Manager Messaging.
 - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition.

The following screen shows the dial patterns used during the compliance test.

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	1	10	11	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	2	5	5	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	5	5	5	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	53	5	5	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	59998	5	5	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	9	12	12	<input type="checkbox"/>			-ALL-	

6.8. Configure SIP Users

During the compliance test, no special users were created for this solution. All users were created prior to the compliance test. However, the steps to configure a user are included.

Add new SIP users for each Trio phone.

To add new SIP users, Navigate to **Users → User Management → Manage Users**. Click **New (not shown)** and provide the following information:

- Identity section
 - **Last Name** – Enter last name of user.
 - **First Name** – Enter first name of user.
 - **Login Name** – Enter an available extension number@sip domain name. The domain name is as defined in **Section 6.1**.

The screenshot shows a web interface for user provisioning. At the top, there are four tabs: 'Identity' (selected), 'Communication Profile', 'Membership', and 'Contacts'. On the left side, there is a sidebar with 'Basic Info' (selected), 'Address', and 'LocalizedName'. The main content area contains the following fields:

- User Provisioning Rule:** A dropdown menu.
- * Last Name:** Text input field containing 'Polycom'.
- Last Name (Latin Translation):** Text input field containing 'Polycom'.
- * First Name:** Text input field containing 'User 1'.
- First Name (Latin Translation):** Text input field containing 'User 1'.
- * Login Name:** Text input field containing '56001@avaya.com'.
- Middle Name:** Text input field containing 'Middle Name Of Us'.

- Communication Profile section
Select **Communication Profile Password** on the left and provide the following information:
 - **Comm-Profile Password** – Enter a numeric value used to logon to Trio
 - **Re-enter Comm-Profile Password** – Repeat numeric password above

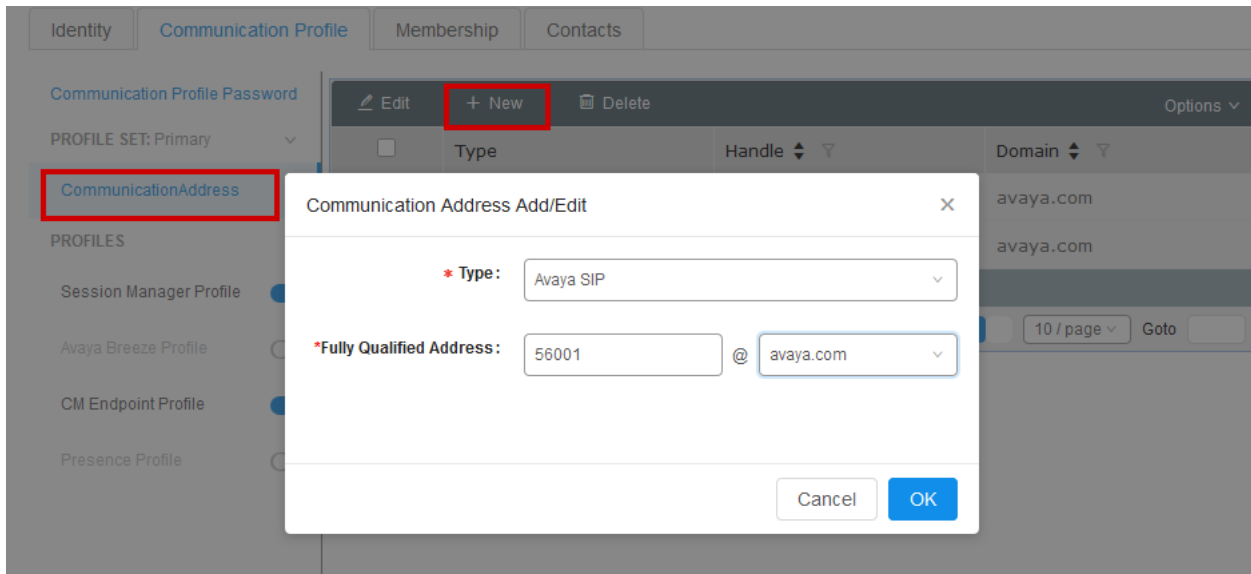
The screenshot displays the Avaya Aura Administration console interface. The 'Communication Profile' tab is selected, and the 'Communication Profile Password' option is highlighted with a red box. A modal dialog titled 'Comm-Profile Password' is open, featuring two input fields: 'Comm-Profile Password' (with masked characters) and 'Re-enter Comm-Profile Password' (with placeholder text). The dialog includes 'Cancel' and 'OK' buttons at the bottom right.

- CommunicationAddress sub-section

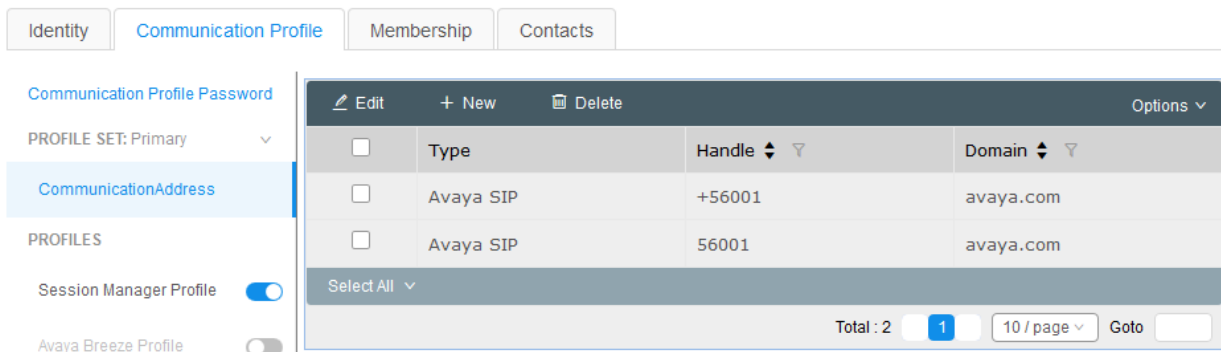
Select **CommunicationAddress** from the left and select **New** to define a **Communication Address** for the new SIP user; provide the following information:

- **Type** – Select **Avaya SIP** using drop-down menu.
- **Fully Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

Click the **Add** button to save the Communication Address for the new SIP user.



- Create another **Communication Address** with + in front. This is required for Communication Manager to send notification correctly for MWI.



- Session Manager Profile section

Toggle the **Session Manager Profile** switch on the left and configure as follows:

- **Primary Session Manager** – Select one of the Session Managers.
- **Origination Application Sequence** – Select Application Sequence defined (configuration not shown) for Communication Manager.
- **Termination Application Sequence** – Select Application Sequence defined (configuration not shown) for Communication Manager.
- **Home Location** – Select Location defined in **Section 6.2** (not shown).

Identity | **Communication Profile** | Membership | Contacts

Communication Profile Password

PROFILE SET: Primary

CommunicationAddress

PROFILES

- Session Manager Profile**
- Emergency Profile
- CM Endpoint Profile
- Presence Profile

SIP Registration

* Primary Session Manager: ⓘ

Secondary Session Manager: ⓘ

Survivability Server: ⓘ

Max. Simultaneous Devices:

Block New Registration When Maximum Registrations Active?:

Application Sequences

Origination Sequence:

Termination Sequence:

- CM Endpoint Profile section

Toggle the **CM Endpoint Profile** switch on the left and configure as follows:

- **System** – Select Managed Element defined in **System Manager** (not shown) for Communication Manager.
- **Use Existing Endpoints** - Leave unchecked to automatically create a new endpoint on Communication Manager when the new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
- **Extension** - Enter same extension number used in this section.
- **Template** – Select template for type of SIP phone. During the compliance test, 9641SIP_DEFAULT_CM_8_0 was selected.

Select **Commit** once done, so save the user.

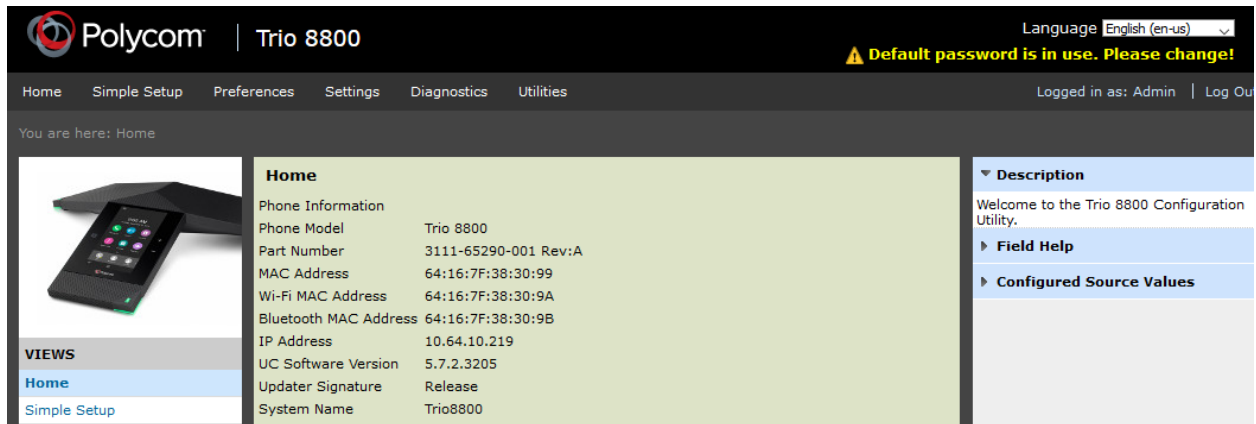
The screenshot shows the 'Communication Profile' configuration page with the following settings:

- System:** cm8 (highlighted with a red box)
- Use Existing Endpoints:**
- Template:** 9641SIP_DEFAULT_CM_Q (highlighted with a red box)
- Security Code:** Enter Security Code
- Voice Mail Number:** (empty field)
- Calculate Route Pattern:**
- Profile Type:** Endpoint
- Extension:** 56001 (highlighted with a red box)
- Set Type:** 9641SIP
- Port:** IP
- Preferred Handle:** Select
- Sip Trunk:** aar

7. Configure Trio

Configuration for Trio phones is done via a web server hosted on the phone. Access the web configuration utility via a browser; <http://<Trio-IP-Address>>. Configuration in this section displays the steps performed on Trio 8800 during compliance test.

Log on using appropriate credentials.



The screenshot shows the Polycom Trio 8800 configuration utility web interface. The page title is "Polycom | Trio 8800". The language is set to "English (en-us)". A warning message states: "Default password is in use. Please change!". The navigation menu includes: Home, Simple Setup, Preferences, Settings, Diagnostics, Utilities. The user is logged in as "Admin" and can click "Log Out".

The main content area is titled "Home" and includes a "Phone Information" section with the following details:

Phone Information	
Phone Model	Trio 8800
Part Number	3111-65290-001 Rev:A
MAC Address	64:16:7F:38:30:99
Wi-Fi MAC Address	64:16:7F:38:30:9A
Bluetooth MAC Address	64:16:7F:38:30:9B
IP Address	10.64.10.219
UC Software Version	5.7.2.3205
Updater Signature	Release
System Name	Trio8800

On the left, there is a "VIEWS" section with "Home" selected and "Simple Setup" as an option. On the right, there is a "Description" section with the text: "Welcome to the Trio 8800 Configuration Utility." Below this are sections for "Field Help" and "Configured Source Values".

Once logged in, Select **Simple Setup**.

Configure as follows:

- Under **SIP Server**, configure the Session Manager SIP IP Address and port in **Address** and **Port**. For TLS use 5061 and for TCP use 5060. In our case 5061 since TLS was used.
- Under **SIP Line Identification**:
 - Type in desired values in **Display Name** and **Label**
 - For **Address** field, type in extension@domain that was configured in **Section 6.8**. E.g., 56001@avaya.com
 - For **Authentication User ID**, type in the extension created in Avaya IP Office from **Section 6.8**
 - For **Authentication Password**, type in the **Login Code** as configured for **Communication Profile Password** in **Section 6.8**.

Once done, select **Save** (not shown).

Home Simple Setup Preferences Settings Diagnostics Utilities

You are here: Simple Setup

Simple Setup

System Name
System Name

Language

Time Synchronization

SIP Server
Address
Port

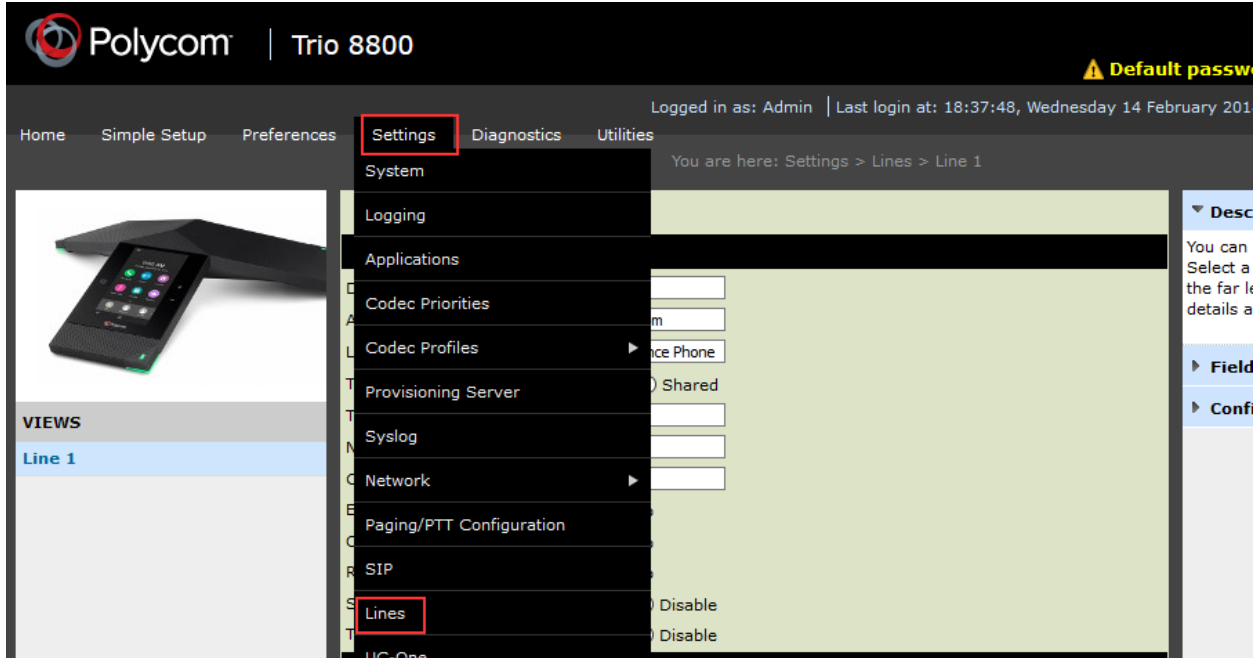
SIP Outbound Proxy

SIP Line Identification
Display Name
Address
Authentication User ID
Authentication Password
Label

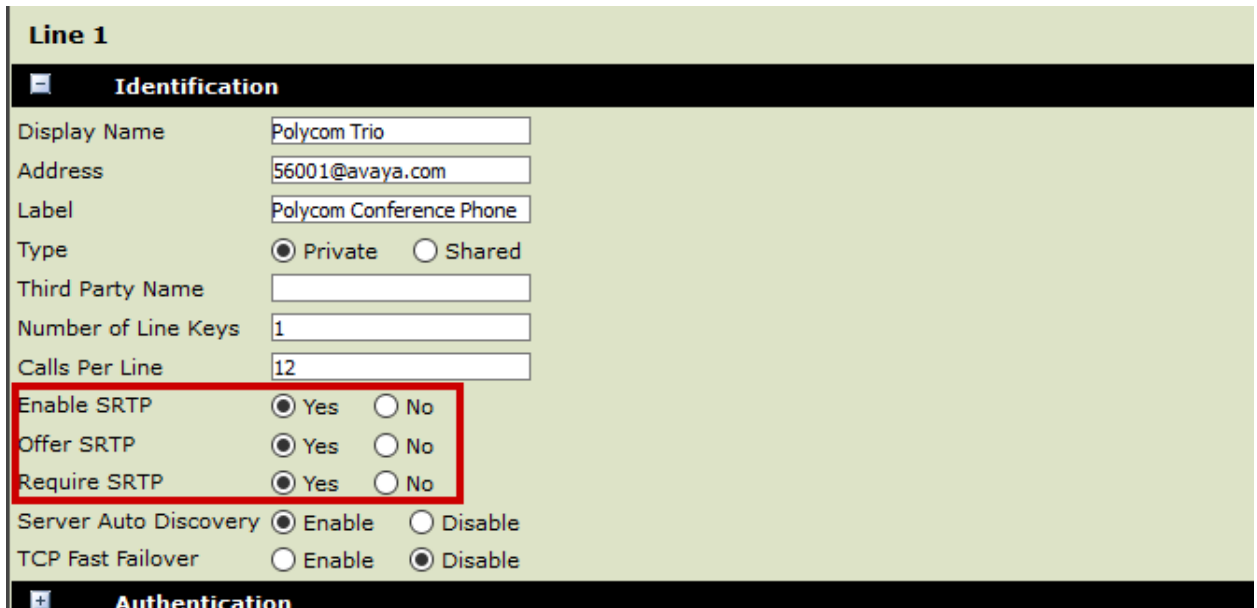
Base Profile

VIEWS
Home
Simple Setup

Navigate to **Settings** → **Lines**



Expand **Identification** and set **Enable SRTP**, **Offer SRTP** and **Require SRTP** to **Yes**.



Expand **Message Center** and configure as follows:

- Type in the extension from **Section 6.8** in **Subscription Address**
- From the drop-down menu for **Callback Mode**, select **Contact**
- For **Callback Contact**, configure the Hunt Group extension that is configured in Communication Manager.

Click **Save**, once done (not shown).

The screenshot shows a configuration interface with a sidebar on the left containing menu items: Server 2, Server 3, Call Diversion, Message Center, and Ring Type. The Message Center section is expanded, showing three input fields: Subscription Address (56001), Callback Mode (Contact), and Callback Contact (59998). These three fields are enclosed in a red rectangular box.

Navigate to **Settings** → **Codec Priorities** to configure codecs. During the compliance test, the following was configured.

The screenshot displays the 'Codec Priorities' configuration page. At the top, there is a navigation bar with 'Home', 'Simple Setup', 'Preferences', 'Settings', 'Diagnostics', and 'Utilities'. Below it, a breadcrumb trail reads 'You are here: Settings > Codec Priorities'. On the left, a sidebar shows 'VIEWS' with options: System, Logging, Applications, Codec Priorities (selected), and Provisioning Server. The main content area is titled 'Codec Priorities' and contains an 'Audio Codec Priority' section. This section has two columns: 'Unused' and 'In use'. The 'Unused' list includes: iLBC (13.33 kbps), iLBC (15.2 kbps), Siren7 (16 kbps), Siren7 (24 kbps), Siren7 (32 kbps), Siren14 (24 kbps), Siren14 (32 kbps), Siren14 (48 kbps), Siren22 (32 kbps), Siren22 (48 kbps), Siren22 (64 kbps), and G.719 (32 kbps). The 'In use' list includes: G.711Mu, G.711A, G.729AB, and G.722. Orange arrow icons are positioned between the two lists. A 'Note' at the bottom states: 'Only codecs with a white background are supported on this platform.'

Please see **Appendix A** for detailed configuration.

8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Trio successfully registers with Session Manager server by following the **Session Manager → System Status → User Registrations** link on the System Manager Web Interface.

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

AST Device Notifications: Reboot Reload Failback As of 10:19 AM												Advanced Search		
3 Items												Filter: Enable		
	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered			
											Prim	Sec	Surv	
<input type="checkbox"/>	Show	56002@avaya.com	User 2	Polycom	DevConnect	10.64.10.220	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Show	56001@avaya.com	User 1	Polycom	DevConnect	10.64.10.219	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Show	---	Station 1	SIP	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

- Place calls to and from Trio and verify that the calls are successfully established with two-way talk path. Verify SIP signaling via the traceSM tool on Session Manager.

51001	SM100	cm8	56001
10:24:25.841	→ INVITE →		(64) sips:51001@avaya.com
10:24:25.843	← Trying →		(64) 100 Trying
10:24:25.844	← Proxy A →		(64) 407 Proxy Authentication Required
10:24:25.883	→ ACK →		(64) sips:51001@avaya.com
10:24:25.883	→ INVITE →		(64) sips:51001@avaya.com
10:24:25.924	← Trying →		(64) 100 Trying
10:24:25.928		→ INVITE →	(64) sips:51001@avaya.com P:imsorig
10:24:25.928		← Trying →	(64) 100 Trying
10:24:25.929		← Session →	(64) 183 Session Progress
10:24:25.932	← Session →		(64) 183 Session Progress
10:24:25.951	→ INVITE →		(64) sips:56001@avaya.com
10:24:25.952	← Trying →		(64) 100 Trying
10:24:25.954	← Proxy A →		(64) 407 Proxy Authentication Required
10:24:25.979	→ ACK →		(64) sips:56001@avaya.com
10:24:25.979	→ INVITE →		(64) sips:56001@avaya.com
10:24:26.020	← Trying →		(64) 100 Trying
10:24:26.025		→ INVITE →	(64) sips:56001@avaya.com P:imsorig
10:24:26.026		← Address →	(64) 484 Address Incomplete
10:24:26.026		← Trying →	(64) 100 Trying
10:24:26.027		→ ACK →	(64) sips:51001@avaya.com
10:24:26.029	← Address →		(64) 484 Address Incomplete
10:24:26.030		← INVITE →	(67) sips:56001@avaya.com P:origdone
10:24:26.032		← Trying →	(67) 100 Trying
10:24:26.036		→ INVITE →	(67) sips:56001@avaya.com P:imsterm
10:24:26.037		← INVITE →	(67) sips:56001@avaya.com P:termdone

- While calls are established, Enter **status trunk <t:r>** command, where **t** is the SIP trunk group configured in **Section 5.6**, and **r** is the trunk group member. On **Page 2**, this will verify whether the call is shuffled or not.

```

CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling  IP Address          Port
  Near-end:  10.64.110.131      : 5061
  Far-end:   10.64.110.135      : 5061
H.245 Near:
H.245 Far:
H.245 Signaling Loc:           H.245 Tunned in Q.931? no

Audio Connection Type: ip-direct      Authentication Type: None
Near-end Audio Loc:                  Codec Type: G.711MU
  Audio    IP Address                Port
  Near-end: 10.64.10.219              : 2232
  Far-end:  10.64.10.202              : 2840

Video Near:
Video Far:
Video Port:
Video Near-end Codec:                Video Far-end Codec:

```

- Continuing from above, navigate to **Page 3** to verify SRTP is used.

```

status trunk 1/1 Page 3 of 3
SRC PORT TO DEST PORT TALKPATH

src port: T00001
T00001:TX:10.64.10.202:2840/g711u/20ms/1-srtp-aescm128-hmac80
T00008:RX:10.64.10.219:2232/g711u/20ms/1-srtp-aescm128-hmac80

dst port: T00008

```

9. Conclusion

Trio was compliance tested with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Trio functioned properly for feature and serviceability. During compliance testing, Trio successfully registered with Avaya Aura® Session Manager, placed and received calls to and from SIP and non-SIP telephones, and executed other telephony features like three-way conference, transfers, hold, etc.

10. Additional References

The following Avaya product documentation can be found at <http://support.avaya.com>

- [1] *Administering Avaya Aura® Communication Manager*, December 2013, Release 6.3, Document Number 03-300509.
- [2] *Administering Avaya® Session Manager*, October 2013, Release 6.3, Issue 3
- [3] *Administering Avaya® System Manager*, October 2013, Release 6.3.Issue 3

Documentation related to Trio can be directly obtained from Polycom.

Appendix A

Following is the exported configuration from Trio 8800.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- Application SIP Arbutus 5.7.2.3205 05-Nov-18 14:52 -->
<!-- Created 12-12-2018 17:34 -->
<!-- Base profile Generic -->
<PHONE_CONFIG>
  <!-- Note: The following parameters have been excluded from the export:
    reg.1.auth.password=""
  -->
  <ALL
    device.prov.serverName.set="1"
    device.prov.ztpEnabled="0"
    device.prov.ztpEnabled.set="1"
    device.set="1"
    dialplan.digitmap=""
    httpd.cfg.secureTunnelEnabled="0"
    log.level.change.sip="0"
    sec.srtp.offer="1"
    sec.srtp.requireMatchingTag="0"
    sec.srtp.sessionParams.noEncrypRTCP.offer="1"
    sec.srtp.sessionParams.noEncrypRTCP.require="1"
    sec.TLS.profileSelection.SIP="ApplicationProfile1"
    sec.TLS.SIP.strictCertCommonNameValidation="0"
    system.name="Trio8800"
    video.codecPref.H261="8"
    video.codecPref.H263="7"
    video.codecPref.H2631998="5"
    video.codecPref.H264.packetizationMode0="6"
    video.codecPref.Xdata="9"
    video.codecPref.XUlpFecUC="10"
    voice.codecPref.G711_A="2"
    voice.codecPref.G711_Mu="1"
    voice.codecPref.G722="5"
    voice.codecPref.G7221.16kbps="10"
    voice.codecPref.G7221.24kbps="9"
    voice.codecPref.G7221.32kbps="8"
    voice.codecPref.G7221_C.24kbps="6"
    voice.codecPref.G7221_C.32kbps="7"
    voice.codecPref.G7221_C.48kbps="4"
    voice.codecPref.G729_AB="3"
    voice.codecPref.Siren14.48kbps="0"
    voice.codecPref.Siren22.64kbps="0"
    msg.mwi.1.callBack="59998"
    msg.mwi.1.callBackMode="contact"
    msg.mwi.1.subscribe="56001"
    reg.1.address="56001@avaya.com"
    reg.1.auth.domain="avaya.com"
    reg.1.auth.loginCredentialType="usernameAndPassword"
    reg.1.auth.userId="56001"
    reg.1.displayName="Polycom Trio"
    reg.1.label="Polycom Conference Phone"
```

```

    reg.1.srtp.offer="1"
    reg.1.srtp.require="1"
<!-- System Manager Root certificate -->
    sec.TLS.customCaCert.1="-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIIOmAtP9ObtnYwDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UE
AwwRU3lzdGVtIE1hbmFnZXIgd0ExDTALBgNVBAsMIBE1HTVQxDjAMBGNVBAoMBUFW
QVlBMB4XDTE4MDgwMTE1NDQzMFOxDTI4MDcyOTE1NDQzMFOwOzEaMBGGA1UEAwWR
U3lzdGVtIE1hbmFnZXIgd0ExDTALBgNVBAsMIBE1HTVQxDjAMBGNVBAoMBUFWQVlB
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsDk8yJPEIsKmcIhdEYe
Y7/y0xPqLzAaaE2cSxGxPmtSxkL1JPBhPZbc+W9qb722/ZbowgHe/GE0ipbpgGjq
sgz2lH6wKCytzTxCoWdHgpNnNMfjANGKvuj8e8nPTbv5D0gXgqMUT7hREDJGAjb/
PCehtn0qpAD2L6bfITFzU1mZzRj2TR37Hp+G+SVaDoTQ553djHpnDoT30IIXM3z
TV3i8v71e+So3avW1pzYsnaLxSEQTY2E+1VjYOFvsRZLVoYUpw4MNFv0o7E3eP+Y
n7leBD0A5aDiE3emFXQKW/Tokyk7MHPi7Ccw1NcbN+vHJ1kE1N1+XWg6ZIEvVXh
CQIDAQABO2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFA89oYPXFTRT
2MFS1rfgbyHR219NMB0GA1UdDgQWBQPPaGD1xU0U9jBUta34G8h0dtfTTAObgNV
HQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAHCch29gg80tvZGChFLdWE2i
sQdQdmSr8fxa2uDSf8WeiJ6YdOiryJa5IH3SDU7dApB7u8GH4AvYNw6aMmTGmeAH
rZy5GoVALEA3dtJmOZzH3A2E3kX0EyQby2NY9eQZ913772ZiyFeWsxARb+uVv8Mv
2morUZ4bD1MNT2biPAsg2YHj6twaiPkfcogDn6Hnz8ad1Crk9E116A496Kvrh3LF
MsXyVZfuYR1hFkcNKbnzg8XDsRdxwKwZWTy1rARe/p7UAWolcK2GMKOsV+XVPqj
9/9bYBD/MaAbiJ/fAMQybyXmoH+C3qpAnbSnL/eebkG2FkwXZCNC6BxkF1kKD2s=
-----END CERTIFICATE-----"
    voIpProt.server.1.address="10.64.110.135"
    voIpProt.server.1.port="5061"
    reg.1.server.1.address="10.64.110.135"
    reg.1.server.1.port="5061"
    reg.1.server.1.transport="TLS"
/>
</PHONE_CONFIG>

```

©2019 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.