



Avaya Solution & Interoperability Test Lab

Application Notes for Biamp Tesira SVC-2 and Avaya Aura[®] Communication Manager and Avaya Aura[®] Session Manager – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Biamp Tesira SVC-2 which was compliance tested with Avaya Aura[®] Communication Manager and Avaya Aura[®] Session Manager.

The overall objective of the interoperability compliance testing is to verify Biamp Tesira SVC-2 functionalities in an environment comprised of Avaya Aura[®] Communication Manager, Avaya Aura[®] Session Manager, various Avaya H.323 and SIP IP Telephones.

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 Biamp Tesira SVC-2 which was compliance tested with Avaya Aura[®] Communication Manager and Avaya Aura[®] Session Manager.

The Tesira SVC-2 enables conferencing over VoIP directly from Tesira SERVER-IO, with two channels of VoIP interface per card. Tesira SVC-2 allows Tesira SERVER-IO to connect directly to IP-based phone systems and eliminate the need for VoIP adapters. Used in conjunction with SEC-4 4-Channel Wideband Acoustic Echo Cancellation Input Cards and STC-2 Dual-Channel Telephone Interface Cards, the Tesira SVC-2 makes Tesira SERVER-IO a powerful, flexible, and affordable telephone conferencing product available. Combined with the STC-2 Card, the Tesira SVC-2 makes it possible to create redundancies within a conferencing system for multi-point conferences and/or back-up to VoIP lines. Up to 6 Tesira SVC-2 can be installed into a single Tesira SERVER-IO unit.

For further details on Tesira SVC-2 configuration steps not covered in this document, consult [4].

2. General Test Approach and Test Results

All test cases were performed manually. The general approach was to place various types of calls to and from Biamp Tesira SVC-2. Biamp Tesira SVC-2 operations such as inbound calls, outbound calls, hold, and Biamp Tesira SVC-2 interactions with Session Manager, Communication Manager, and Avaya SIP and H.323 telephones were verified. For serviceability testing, failures such as cable pulls and resets were applied.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the interoperability between Biamp Tesira SVC-2, Session Manager, and Communication Manager. The serviceability testing introduced failure scenarios to see if Biamp Tesira SVC-2 could resume after failure.

2.2. Test Results

All test cases passed.

2.3. Support

Technical support for Biamp Tesira SVC-2 solution can be obtained by contacting Biamp at:

- <http://www.biamp.com/support/index.aspx>
- (800)-826-1457

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya S8300D Server, an Avaya G450 Media Gateway, a Session Manager server, and Biamp Tesira SVC-2. The solution described herein is also extensible to other Avaya Servers and Media Gateways. Avaya S8720 Servers with an Avaya G650 Media Gateway was included in the test to provide an inter-switch scenario. For completeness, Avaya SIP Enablement Services, Avaya 9600 Series H.323 IP Telephones, Avaya 9600 Series SIP IP Telephones, and Avaya 6400 Series Digital Telephones, are included in Figure 1 to demonstrate calls between the Biamp Tesira SVC-2 and Avaya SIP, H.323, and digital telephones.

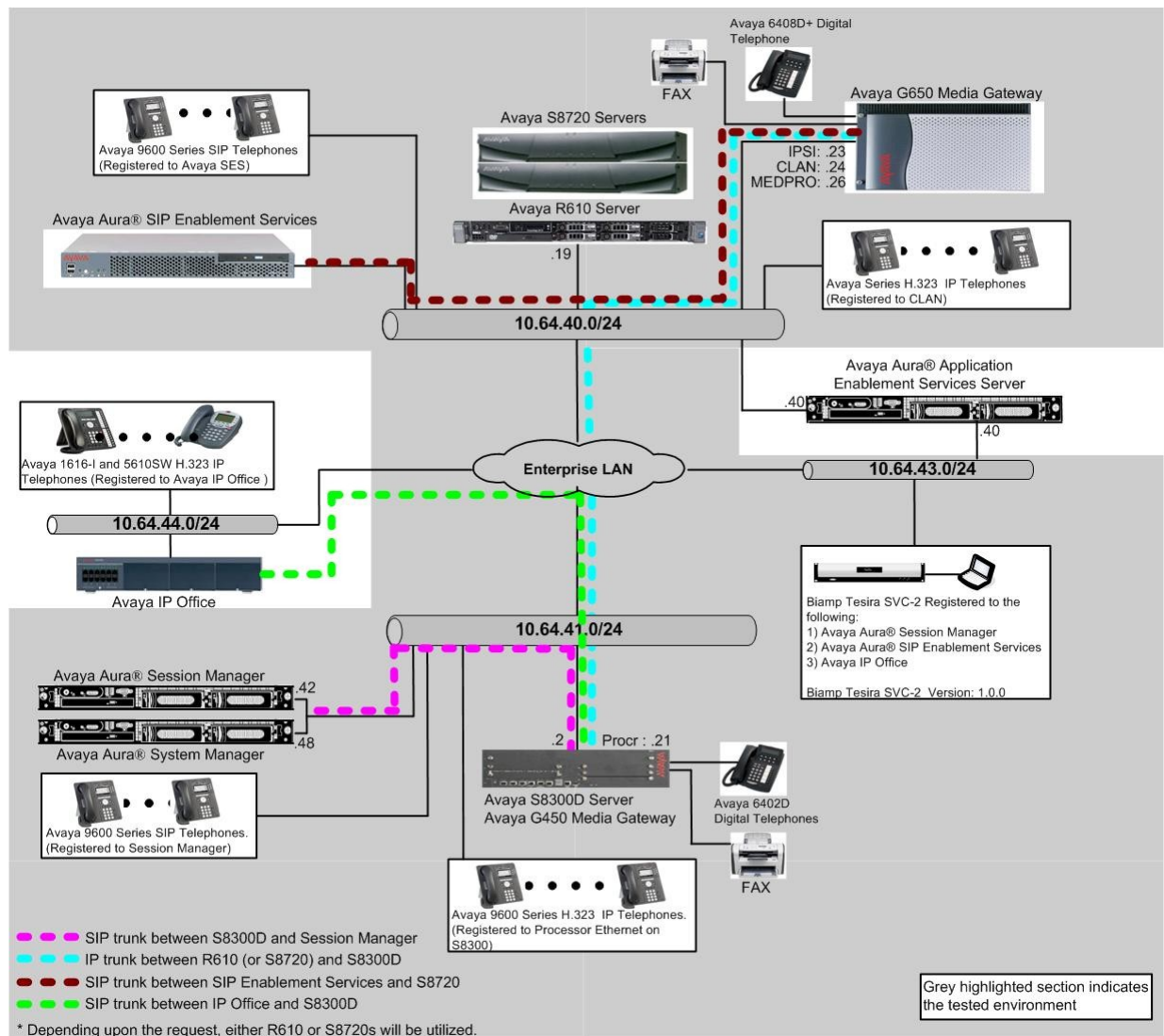


Figure 1: Test Configuration of Biamp Tesira SVC-2

4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0.1(R016x.00.1.510.1) w/ patch 00.1.510.1-19303
Avaya Aura® System Manager		6.1.5.0
Avaya Aura® Session Manager		6.1.5.0
Avaya S8720 Servers with Avaya G650 Media Gateway (<i>used for inter-switch test scenarios</i>)		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya Aura® SIP Enablement Services		5.2.1
Avaya 9600 Series IP Telephones		
	9620 (H.323)	3.1
	9630 (H.323)	3.1
	9650 (H.323)	3.1
Avaya 9600 Series SIP Telephones		
	9620 (H.323)	2.6.4
	9630 (H.323)	2.6.4
	9650 (H.323)	2.6.4
Avaya 6408D+ Digital Telephone		-
Biamp Tesira SVC-2		1.0.0
Biamp Tesira		1.0.0
Linux		2.6.32.28-BIAMP

5. Configure 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. Biamp Tesira SVC-2 and other SIP telephones are configured as off-PBX telephones in Communication Manager.

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 11
OPTIONAL FEATURES		
G3 Version: V16	Software Package: Enterprise	
Location: 2	System ID (SID): 1	
Platform: 28	Module ID (MID): 1	
		USED
Platform Maximum Ports: 6400		161
Maximum Stations: 2400		34
Maximum XMOBILE Stations: 2400		0
Maximum Off-PBX Telephones - EC500: 9600		0
Maximum Off-PBX Telephones - OPS: 9600		13
Maximum Off-PBX Telephones - PBFMC: 9600		0
Maximum Off-PBX Telephones - PVFMC: 9600		0
Maximum Off-PBX Telephones - SCCAN: 0		0
Maximum Survivable Processors: 313		1

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 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks: 4000		35
Maximum Concurrently Registered IP Stations: 2400		3
Maximum Administered Remote Office Trunks: 4000		0
Maximum Concurrently Registered Remote Office Stations: 2400		0
Maximum Concurrently Registered IP eCons: 68		0
Max Concur Registered Unauthenticated H.323 Stations: 100		0
Maximum Video Capable Stations: 2400		2
Maximum Video Capable IP Softphones: 2400		1
Maximum Administered SIP Trunks: 4000		50
Maximum Administered Ad-hoc Video Conferencing Ports: 4000		0
Maximum Number of DS1 Boards with Echo Cancellation: 80		0
Maximum TN2501 VAL Boards: 10		0
Maximum Media Gateway VAL Sources: 50		1
Maximum TN2602 Boards with 80 VoIP Channels: 128		0
Maximum TN2602 Boards with 320 VoIP Channels: 128		0
Maximum Number of Expanded Meet-me Conference Ports: 300		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** when configuring an IP network region to specify which codec sets may be used within and between network regions.

```
change ip-codec-set 1
```

Page 1 of 2

IP Codec Set

Codec Set: 1

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

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: Authoritative Domain: avaya.com
Name:
MEDIA PARAMETERS
  Codec Set: 1
  Intra-region IP-IP Direct Audio: yes
  Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048
  UDP Port Max: 3329
  IP Audio Hairpinning? n
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
H.323 IP ENDPOINTS
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
AUDIO RESOURCE RESERVATION PARAMETERS
  RSVP Enabled? n
```

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 IP address.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
CLAN	10.64.40.24	
IPOffice	10.64.44.21	
SES	10.64.40.41	
SM-1	10.64.41.42	
SM-2	10.64.21.31	
default	0.0.0.0	
procr	10.64.41.21	
procr6	::	

5.5. Configure SIP Signaling

This section describes the steps for administering a signaling group in Communication Manager for signaling 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** as displayed in **Section 5.4**.
- **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**.

add signaling-group 92		Page 1 of 1
		SIGNALING GROUP
Group Number: 92	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		SIP Enabled LSP? n
IP Video? y	Priority Video? n	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM-1	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
	Far-end Secondary Node Name:	
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? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

5.6. Configure SIP Trunk

This section describes the steps for administering a trunk group in Communication Manager for trunking 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.
- **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.

```
add trunk-group 92                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 92                                     Group Type: sip          CDR Reports: y
Group Name: SM_41_42                                COR: 1                 TN: 1                 TAC: 1092
Direction: two-way                                Outgoing Display? y
Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                                Auth Code? n
                                           Member Assignment Method: auto
                                           Signaling Group: 92
                                           Number of Members: 10
```

5.7. Configure SIP Endpoint

This section displays an extension created from Session Manager.

```
display station 72032                                Page 1 of 6
                                     STATION
Extension: 72032                                Lock Messages? n        BCC: 0
Type: 9620SIP                                Security Code: 123456    TN: 1
Port: S00107                                Coverage Path 1: 99      COR: 1
Name: Biamp-2                                Coverage Path 2:         COS: 1
                                           Hunt-to Station:
STATION OPTIONS
Location:                                Time of Day Lock Table:
Loss Group: 19                                Message Lamp Ext: 72032
Display Language: english
Survivable COR: internal
Survivable Trunk Dest? y                    IP SoftPhone? n
                                           IP Video? n
```


6. Configure Avaya Aura[®] Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is comprised of two functional components: The Session Manager server and the 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.

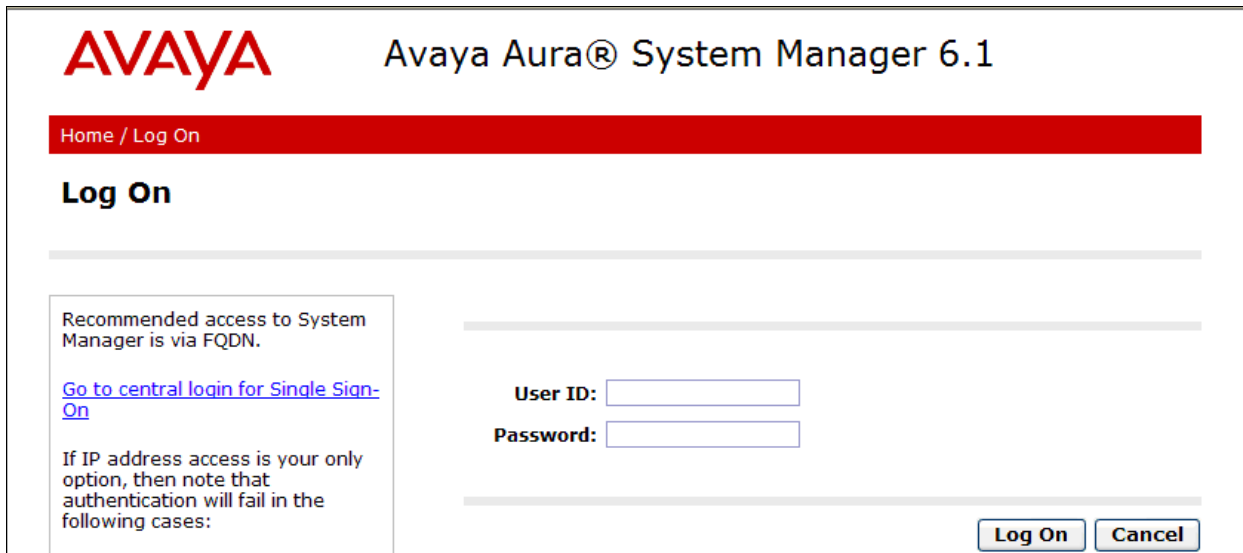
This section assumes that Session Manager and System Manager have been installed, and network connectivity exists between the two platforms.

The following steps describe for configuring Session Manager.

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Applications
- Application Sequence
- User Management
- TLS certificate between 3rd party endpoint and Session Manager

6.1. Configure SIP Domain

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

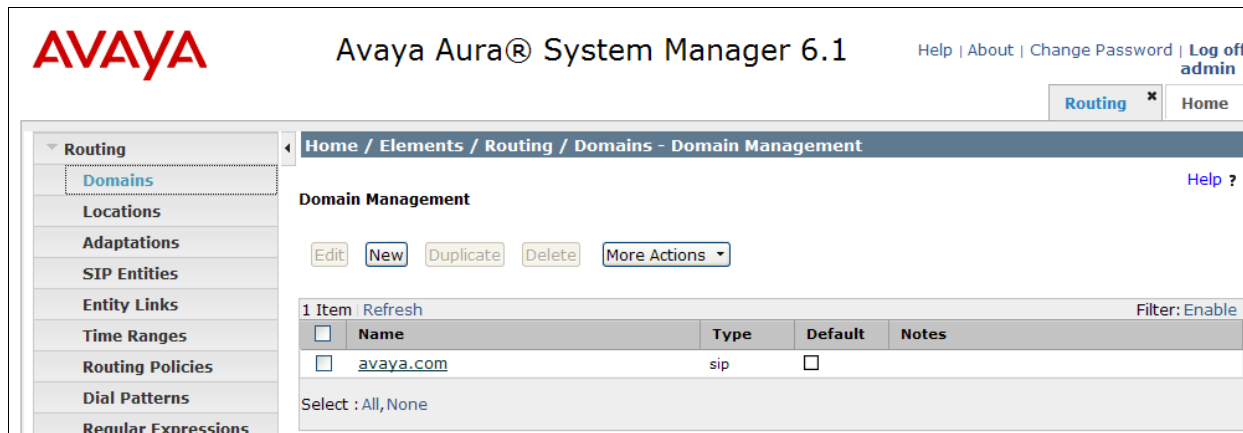


The screenshot shows the Avaya Aura® System Manager 6.1 login page. At the top is the Avaya logo and the title "Avaya Aura® System Manager 6.1". Below this is a red navigation bar with "Home / Log On". The main heading is "Log On". On the left, a box contains the text: "Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases:". To the right of this box are input fields for "User ID:" and "Password:". At the bottom right are "Log On" and "Cancel" buttons.

Navigate to **Elements→Routing→Domains** and click on the **New** button to create a new SIP Domain (screen not shown). Enter the following values and use defaults for the 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 shows the Domains page used during the compliance test.



The screenshot shows the "Domain Management" page in Avaya Aura® System Manager 6.1. The top navigation bar includes "Help | About | Change Password | Log off admin". A breadcrumb trail reads "Home / Elements / Routing / Domains - Domain Management". On the left is a sidebar menu with "Routing" expanded, showing "Domains" as the selected item. The main content area has a "Domain Management" heading and buttons for "Edit", "New", "Duplicate", "Delete", and "More Actions". Below these is a table with one item, "avaya.com", of type "sip". The table has columns for "Name", "Type", "Default", and "Notes". At the bottom, it says "Select : All, None".

Name	Type	Default	Notes
avaya.com	sip	<input type="checkbox"/>	

6.2. Configure Locations

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

Navigate to **Routing→Locations**, and click on the **New** button to create a new SIP Entity location (screen not shown).

General section

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

- Enter a descriptive Location in the **Name** field (e.g. **.41 Subnet**).
- Enter a description in the **Notes** field if desired.

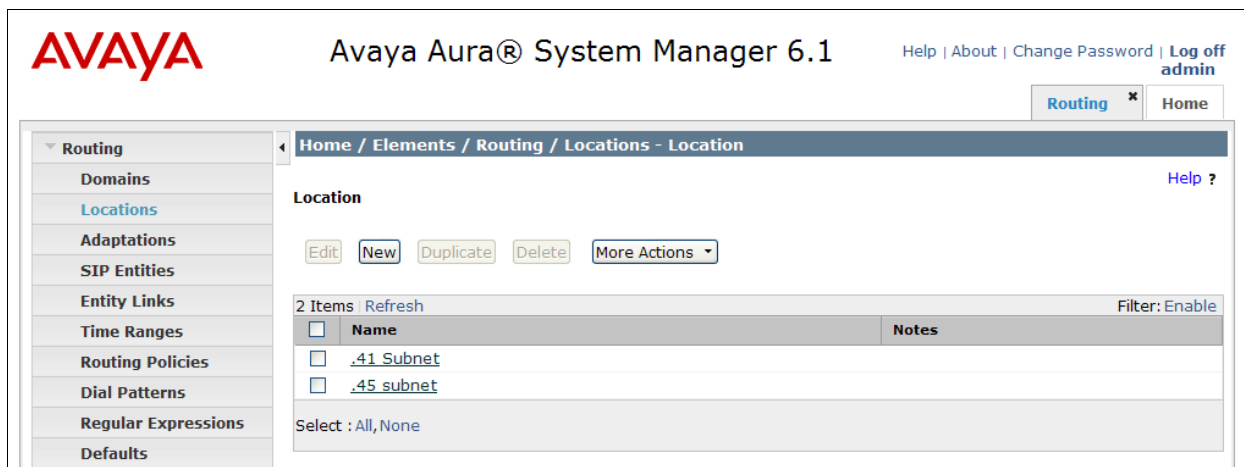
Location Pattern section

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

- The IP address information for the **IP address Pattern** (e.g. **10.64.41.***).
- A description in the **Notes** field if desired.

Repeat these 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.

Repeat all the steps for each new Location. The following screen shows the Location page used during the compliance test.



6.3. Configure SIP Entities

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

- Session Manager itself
- Communication Manager (Avaya S8300D Server)

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

General section

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the IP address of the signaling interface on each:
 - Communication Manager
 - Session Manager virtual SM-100
- 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.

Click on the **Commit** button to save each SIP entity. The following screen shows the SIP Entities page used during the compliance test.

Repeat all the steps for each new entity.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below the navigation bar, there is a breadcrumb trail: 'Home / Elements / Routing / SIP Entities - SIP Entities'. The main content area is titled 'SIP Entities' and includes buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. A table displays 4 items with columns for 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. The table contains two entries: 'S8300D' with IP address '10.64.41.21' and type 'CM', and 'SessionManager' with IP address '10.64.40.42' and type 'Session Manager'. The 'SessionManager' entry has a note: 'SessionManager in D4H26'. The table also includes a 'Filter: Enable' option and a 'Select: All, None' option.

Name	FQDN or IP Address	Type	Notes
S8300D	10.64.41.21	CM	
SessionManager	10.64.40.42	Session Manager	SessionManager in D4H26

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.

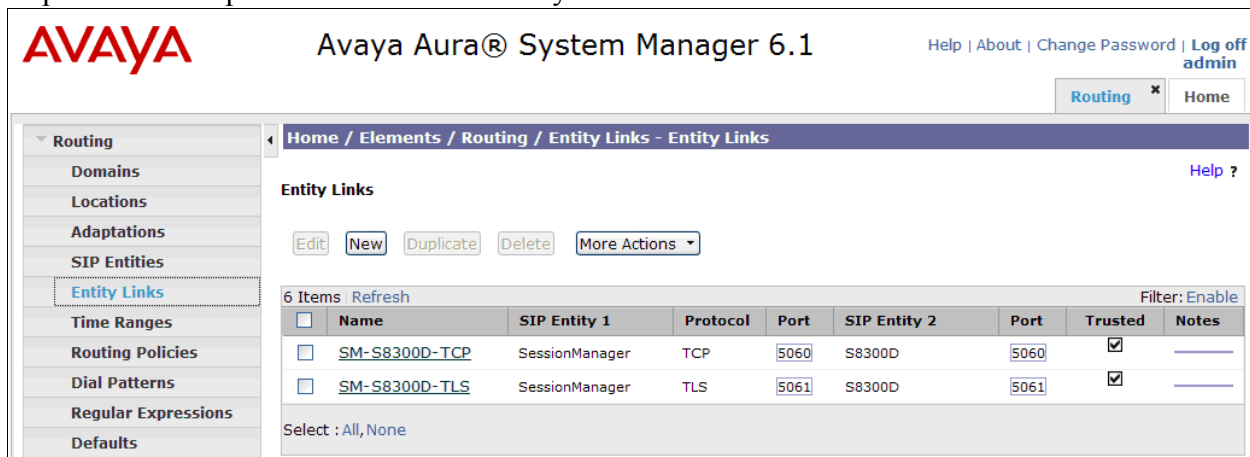
- Session Manager ⇔ Communication Manager (Avaya S8300D Server)

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

- **Name:** Enter a descriptive name.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 6.3** (e.g. **SessionManager**).
- 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 the Communication Manager SIP Entity created in **Section 6.3** (e.g. **S8300D**).
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.

Click on the **Commit** button to save each Entity Link definition. The following screen shows an Entity Links page used during the compliance test.

Repeat all the steps for each new SIP Entity Link



The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for Help, About, Change Password, and Log off admin. The main navigation menu on the left lists various configuration areas, with "Entity Links" selected under the "Routing" section. The main content area displays the "Entity Links" configuration page, which includes a breadcrumb trail "Home / Elements / Routing / Entity Links - Entity Links" and a "Help ?" link. Below the breadcrumb trail, there are buttons for "Edit", "New", "Duplicate", "Delete", and "More Actions". A table lists 6 items, with a "Refresh" button and a "Filter: Enable" dropdown. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. Two items are visible: "SM-S8300D-TCP" and "SM-S8300D-TLS", both configured with "SessionManager" as SIP Entity 1, "S8300D" as SIP Entity 2, and ports "5060" and "5061" respectively. Both items are marked as "Trusted" (checked box) and have empty "Notes" fields. At the bottom of the table, there is a "Select : All, None" option.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	SM-S8300D-TCP	SessionManager	TCP	5060	S8300D	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM-S8300D-TLS	SessionManager	TLS	5061	S8300D	5061	<input checked="" type="checkbox"/>	

6.5. Time Ranges

Time Ranges define 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 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 the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". Below the navigation bar, there are tabs for "Routing" (selected) and "Home". The main content area is titled "Time Ranges" and includes a "Help ?" link, "Commit", and "Cancel" buttons. A table with the following columns is displayed: "Name", "Mo", "Tu", "We", "Th", "Fr", "Sa", "Su", "Start Time", "End Time", and "Notes". The table contains one row with the name "24/7", all days of the week checked, and start/end times of "00:00" and "23:59" respectively. A "Filter: Enable" link is also present. At the bottom, there is a "* Input Required" message and "Commit" and "Cancel" buttons.

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
* 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	

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:

- Inbound calls to Communication Manager.

To add a Routing Policy, navigate to **Routing → Routing Policies** and click on the **New** button on the right (screen not shown). 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 a SIP Entity that will be the destination for this call.
- 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 Policy used for Communication Manager during the compliance test.

The screenshot displays the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for Help, About, Change Password, and Log off admin. A breadcrumb trail shows 'Home / Elements / Routing / Routing Policies - Routing Policies'. The left sidebar contains a tree view with categories like Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, and Routing Policies (which is highlighted). The main content area is titled 'Routing Policies' and includes buttons for Edit, New, Duplicate, Delete, and More Actions. Below these buttons is a table with 3 items. The table has columns for Name, Disabled, Destination, and Notes. One policy is listed: 'To S8300D' with the destination 'S8300D'. A 'Filter: Enable' option is visible on the right. At the bottom of the table, it says 'Select : All, None'.

Name	Disabled	Destination	Notes
To S8300D	<input type="checkbox"/>	S8300D	

6.7. Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In the compliance test, the following dial patterns are defined from Session Manager.

- 720 – endpoints in Avaya S8300D Server

To add a Dial Pattern, select **Routing → Dial Patterns** and click on the **New** button (not shown) on the right pane. Provide the following information:

General section

- Enter a unique pattern in the **Pattern** field (e.g. **720**).

- 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** drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.

Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the box for the appropriate Originating Locations, and Routing Policies (see **Section 6.6**) that pertain to this Dial Pattern.
 - Select the Originating Location to apply the selected routing policies to **All**.
 - Select Routing Policies to **To S8300D**.
 - 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 pattern used for **720xx** during the compliance test. Repeat steps for the remaining Dial Patterns.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 720

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: avaya.com

Notes: SIP and H.323 on S8300D

Additional notes with max. 255 characters.

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To S8300D	0	<input type="checkbox"/>	S8300D	Route to S8300D

6.8. Configure Managed Elements

To define a new Managed Element, navigate to **Elements → Inventory → Manage Elements**. Click on the **New** button (not shown) to open the **New Entities Instance** page.

In the **New Entities Instance** Page

- In the **Type** field, select **CM** using the drop-down menu and the **New CM Instance** page opens (not shown).

In the **New CM Instance Page**, provide the following information:

- Application section
 - **Name** – Enter name for Communication Manager (Evolution Server).
 - **Description** - Enter description if desired.
 - **Node** – Enter IP address of the administration interface. During the compliance test, the **procr** IP address (10.64.41.21) was utilized.

The screenshot shows a web-based configuration interface with two tabs: "Application" (active) and "Attributes". Under the "Application" tab, there is a section titled "Application" with a dropdown arrow. Below this, there are four fields:

- * Name**: A text input field containing "Element-S8300D".
- * Type**: A dropdown menu showing "CM".
- Description**: A text area containing "S8300D in D4H26".
- * Node**: A text input field containing "10.64.41.21".

- Attributes section
System Manager uses the information entered in this section to log into Communication Manager using its administration interface. Enter the following values and use default values for remaining fields.
 - **Login** – Enter login used for administration access
 - **Password** – Enter password used for administration access
 - **Confirm Password** – Repeat value entered in above field
 - **Is SSH Connection** – Check the box
 - **Port** – Verify **5022** is set

Application *

Attributes *

SNMP Attributes ▾

* Version
☒ None
☐ V1
☐ V3

Attributes ▾

* Login

Password

Confirm Password

Is SSH Connection
☒

* Port

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled
☐

ASG Key

Confirm ASG Key

Location

Click **Commit** (not shown) to save the element. The following screen shows the element created, **Element-S8300D**, during the compliance test.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Inventory](#) x
 [Routing](#) x
 [Home](#)

Inventory

Manage Elements

Discovered Inventory

Discovery Management

Synchronization

Home / Elements / Inventory / Manage Elements - Manage Elements

Manage Elements

Entities

View

Edit

New

Delete

More Actions ▾

3 Items

Refresh

Show ALL ▾

Filter: Enable

<input type="checkbox"/>	Name	Node	Type	Version	Description
<input type="checkbox"/>	Element-DellCM	10.64.40.24	CM		DellCM in D4H26
<input type="checkbox"/>	Element-S8300D	10.64.41.21	CM		S8300D in D4H26
<input type="checkbox"/>	Element-SessionManager	10.64.40.43	Session Manager		SessionManager in D4H26

Select : All, None

6.9. Configure Applications

To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications**. Click **New** (not shown) to open the Applications Editor page:

- Application Editor section
 - **Name** – Enter name for the application.
 - **SIP Entity**–Select the SIP Entity for Communication Manager defined in **Section 6.3**.
 - **CM System for SIP Entity** –Select the name of the Managed Element defined for Communication Manager in **Section 6.8**.
 - **Description**– Enter description if desired.

The screenshot shows the 'Application' editor form. It has the following fields and controls:

- Name:** A text input field containing 'App-S8300D'.
- SIP Entity:** A dropdown menu showing 'S8300D'.
- CM System for SIP Entity:** A dropdown menu showing 'Element-S8300D', a 'Refresh' button, and a link 'View/Add CM Systems'.
- Description:** An empty text input field.

- Leave the fields in the Application Attributes (optional) section blank.

Click the **Commit** button (not shown) to save the Application. The screen below shows the Application, **App-S8300D**, defined for Communication Manager.

The screenshot shows the 'Avaya Aura® System Manager 6.1' interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, and Application Configuration. The main content area is titled 'Applications' and includes a breadcrumb trail: 'Home / Elements / Session Manager / Application Configuration / Applications - Applications'. Below the title, there is a description: 'This page allows you to add, edit, or remove applications for available SIP Entities.' and a section for 'Application Entries' with 'New', 'Edit', and 'Delete' buttons. A table lists the existing applications:

<input type="checkbox"/>	Application Name	SIP Entity	Description
<input type="checkbox"/>	App-R610	R610	
<input type="checkbox"/>	App-S8300D	S8300D	


Below the table, there is a 'Select' dropdown menu set to 'All, None' and a 'Filter: Enable' option.

6.10. Define Application Sequence



Navigate to **Elements** → **Session Manager** → **Application Configuration** → **Application Sequences**. Click **New** (not shown) and provide the following information:

- Sequence Name section
 - **Name** – The name for the application.
 - **Description** – Enter description, if desired.

Application Sequence
***Name**
Description

- Available Applications section
 - Click  icon associated with the Application for Communication Manager defined in **Section 6.9** to select this application.
 - Verify a new entry is added to the Applications in this Sequence table as shown below.

Click the **Commit** button (not shown) to save the new Application Sequence.

Applications in this Sequence					
<div>Move First Move Last Remove</div>					
1 Item					
<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	  	App-S8300D	S8300D	<input checked="" type="checkbox"/>	
Select : All, None					

The screen below shows the Application Sequence, **AppSeq-S8300D**, defined during the compliance test.

6.11. Configure User

When adding new SIP user, use the option to automatically generate the SIP station in Communication Manager, after adding a new SIP user.

To add new SIP users, Navigate to **Home → Users → User Manage → Manage Users**. Click **New** and provide the following information:

- Identity section
 - **Last Name** – Enter last name of user.
 - **First Name** – Enter first name of user.
 - **Login Name** – Enter extension number@sip domain. The sip domain is defined as Authoritative Domain in **Section 5.2**.
 - **Authentication Type** – Verify **Basic** is selected.
 - **Password** – Enter password to be used to log into System Manager.
 - **Confirm Password** – Repeat value entered above.

Identity *	Communication Profile *	Membership	Contacts
<p>Identity ▾</p> <p>* Last Name: <input type="text" value="72032"/></p> <p>* First Name: <input type="text" value="72032"/></p> <p>Middle Name: <input type="text"/></p> <p>Description: <input type="text"/></p> <p>* Login Name: <input type="text" value="72032@avaya.com"/></p> <p>* Authentication Type: <input type="text" value="Basic"/></p> <p>* Password: <input type="password" value="••••••••"/></p> <p>* Confirm Password: <input type="password" value="••••••••"/></p> <p>Localized Display Name: <input type="text" value="Biamp-1"/></p> <p>Endpoint Display Name: <input type="text" value="Biamp-1"/></p> <p>Honorific: <input type="text"/></p> <p>Language Preference: <input type="text" value="English"/></p> <p>Time Zone: <input type="text" value="{ -7:0 } Mountain Time (US & Canada): Chihuahua, La Paz"/></p>			

- Communication Profile section
 - **Communication Profile Password** – Type Communication profile password in this field
 - **Confirm Password** – Repeat value entered above.

Identity * Communication Profile * Membership Contacts

Communication Profile ▾

Communication Profile Password: ●●●●●

Confirm Password: ●●●●●

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary

Default : ☒

- Communication Profile sub-section
 - **Fully Qualified Address** – Enter the extension of the user
 - Click **Add** button

Communication Address ▾

New Edit Delete

	Type	Handle	Domain
No Records found			

Type: Avaya SIP ▾

* Fully Qualified Address: 72032 @ avaya.com ▾

Add Cancel

- Session Manager Profile section
 - **Primary Session Manager** – Select one of the Session Managers.
 - **Secondary Session Manager** – Select **(None)** from drop-down menu.
 - **Origination Application Sequence** – Select Application Sequence defined in **Section 6.10** for Communication Manager.

- **Termination Application Sequence** – Select Application Sequence defined in **Section 6.10** for Communication Manager.
- **Survivability Server** – Select **(None)** from drop-down menu.
- **Home Location** – Select Location defined in **Section 6.2**.

☒ **Session Manager Profile**

* **Primary Session Manager**

SessionManager

Secondary Session Manager

(None)

Origination Application Sequence

AppSeq-S8300D

Termination Application Sequence

AppSeq-S8300D

Survivability Server

(None)

* **Home Location**

41-subnet

Primary	Secondary	Maximum
15	0	15

Primary	Secondary	Maximum

- Endpoint Profile section
 - **System** – Select Managed Element defined in **Section 6.8**.
 - **Profile Type** – Select **Endpoint**.

- **Use Existing Endpoints** - Leave unchecked to automatically create new endpoint when 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
- **Security Code** – Enter numeric value used to logon to SIP telephone. (**Note:** this field must match the value entered for the Shared Communication Profile Password field.
- **Port** – Select **IP** from drop down menu
- **Voice Mail Number** – Enter **Pilot Number** for Avaya Modular Messaging if installed. Or else, leave field blank. This feature is not used during the compliance test.
- **Delete Station on Unassign of Endpoint** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.

☒ **Endpoint Profile**

* **System**

* **Profile Type**

Use Existing Endpoints ☐

* **Extension**

* **Template**

Set Type

Security Code

* **Port**

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☒

The following describes steps to configure a 3rd party endpoint (Biamp Tesira SVC-2) to utilize TLS protocol.

- ```
-----BEGIN CERTIFICATE-----
MIICqDCCAhGgAwIBAgIJAI1AR5p845/8MA0GCSqGSIb3DQEBBQUAMG0xETAPBgNV
BAMTCHdlc3RsYWtlMQ8wDQYDVQIQIEWZPcmVnb24xChZAJBgNVBAYTAlVTMSIwIAYJ
KoZIHvcNAQKBFBH3XZN0bGFRZUBiaWFtcGMuY29tMRYwFAYDVQQKEw1CaWftcCBT
eXN0ZW1zMBA4XDTEhMDgxMjIxMjg3OVV0XDTEYMDgxMTIxMjg3OVVwbTERMA8GA1UE
AxMId2VzdGxha2UxZDANBgNVBAgTBk9yZWdwb3JlEAMaGA1UEBhMCVVMxIjAgBgkq
hkiG9w0BCQEWED3dlc3RsYWtlQGJpYWlwYy5jb20xChZAJBgNVBAoTUDJpYWlwIFN5
c3RlbnBMwGZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALggAdFrDOckgQ9Sg/VF
SPTccuRp/LQNB2J9OmU8tBroDSbb048iH49RjkoESGivYQZHZ9JMUkWZLCHdixpPO
utp0f2oeS/+9s/jSTHqBSOI9xVfAXkDUvNphmMD6CsTKyNo6T5npUNp4ddYeP2Ey
j0ZjhqarQvHsL/DgFF2orFOH1AGMBAAGjYUDBOMAwGSIUdEwGFAMBA6f8wHgYDVR0B
BBcwFYETd2Gxha2VAYmlhbHB3LmNvbTAEBgNVHRIEFzAVGvRN3XZN0bGFRZUBi
aWftcGMuY29tMA0GCSqGSIb3DQEBBQUAA4GBAIAKF6GN0ZyWxksWGTATez3gGyKiF
J99i1V+m4WY58+fLEmKgKZtA8jMayGQRfDsPXIVIn9NzIOjgB15nEUXHBXPT00wp
VVC6vrcECyTAkzw7yiYAT200ZhoSFuQ4JKutws39jzZLmOf2V1o3jzOTuwtS0f1o
i08Sjew01eJE1n2B
-----END CERTIFICATE-----
```

- In Session Manager, navigate to **Elements → Inventory → Manage Elements**. Click the Session Manager and select **More Actions → Configure Trusted Certificates**. From the Trusted Certificates page, select **Add**.

**Trusted Certificates**

View **Add** Export Remove

22 Items Refresh Filter: Enable

| <input type="checkbox"/> | Store Description                                    | Store Type         | Subject Name                                                                                           |
|--------------------------|------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US         |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=avaya development team, OU=UK Engineering, O=avaya, L=Cardiff, ST=S Wales, C=UK                     |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | EMAILADDRESS=igonzales@avaya.com, OU=EMMC, O=AVAYA, L=Andover, ST=MA, C=US                             |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=Avaya                                                                                               |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=SCCAN Server Root CA, OU=Seamless Converged Communication Across Networks, O="Motorola, Inc.", C=US |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=Avaya Call Server, OU=Media Server, O=Avaya Inc., C=US                                              |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=Avaya Product Root CA, OU=Avaya Product PKI, O=Avaya Inc., C=US                                     |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | O=Biamp Systems, EMAILADDRESS=westlake@biamp.com, C=US, ST=Oregon, CN=westlake                         |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | O=AVAYA, OU=MGMT, CN=default                                                                           |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=Avaya Manufacturing Subordinate CA, OU=Avaya Product PKI, O=Avaya Inc., C=US                        |

Select : All, None < Previous Page 1 of 3 Next >

- In the **Add Trusted Certificate** page, select **Import from file**. Using the Browse provide the path to the RootCA Certificate. Click the **Retrieve Certificate**.

### Add Trusted Certificate

CommitCancel

---

Select Store Type to add trusted certificate All

☐ Import from existing  
☒ Import from file  
☐ Import as PEM Certificate  
☐ Import using TLS

\* Please select a file H:\Biamp\user-calist.pem Browse...

You must click the Retrieve certificate button and review the certificate details before you can continue. Retrieve Certificate

CommitCancel

- The RootCA Certificate should be visible in the **Trusted Certificate** page.

### Trusted Certificates

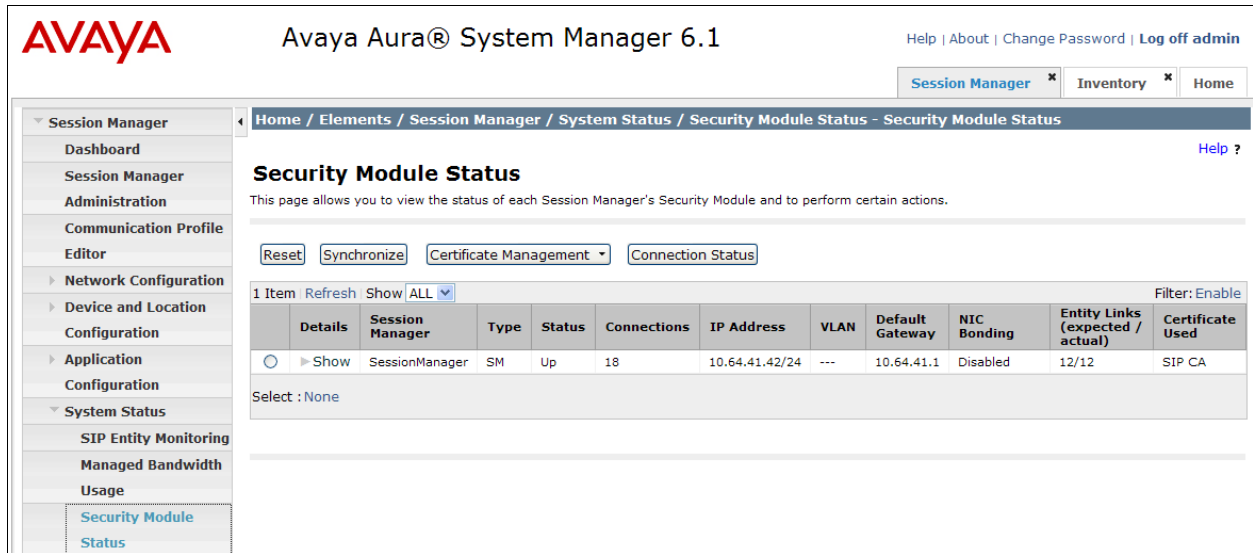
ViewAddExportRemove

22 Items Refresh Filter: Enable

|                          | Store Description                                    | Store Type         | Subject Name                                                                                           |
|--------------------------|------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US         |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=avaya development team, OU=UK Engineering, O=avaya, L=Cardiff, ST=S Wales, C=UK                     |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | EMAILADDRESS=igonzaes@avaya.com, OU=EMMC, O=AVAYA, L=Andover, ST=MA, C=US                              |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=Avaya                                                                                               |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=SCCAN Server Root CA, OU=Seamless Converged Communication Across Networks, O="Motorola, Inc.", C=US |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=Avaya Call Server, OU=Media Server, O=Avaya Inc., C=US                                              |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=Avaya Product Root CA, OU=Avaya Product PKI, O=Avaya Inc., C=US                                     |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | O=Biamp Systems, EMAILADDRESS=westlake@biampc.com, C=US, ST=Oregon, CN=westlake                        |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | O=AVAYA, OU=MGMT, CN=default                                                                           |
| <input type="checkbox"/> | Used for validating TLS client identity certificates | SM_SECURITY_MODULE | CN=Avaya Manufacturing Subordinate CA, OU=Avaya Product PKI, O=Avaya Inc., C=US                        |

Select : All, None < Previous Page 1 of 3 Next >

- Navigate to **Elements** → **Session Manager** → **System Status** → **Security Module Status**.



**AVAYA** Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Session Manager](#) ✕ [Inventory](#) ✕ [Home](#)

[Home](#) / [Elements](#) / [Session Manager](#) / [System Status](#) / [Security Module Status](#) - Security Module Status [Help ?](#)

### Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

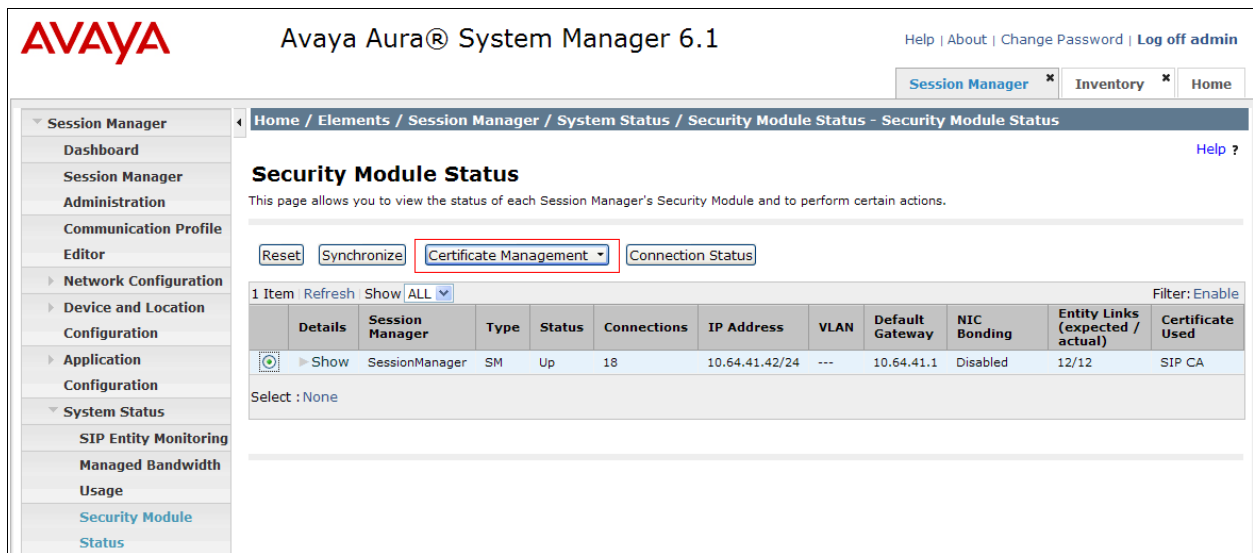
[Reset](#) [Synchronize](#) [Certificate Management](#) ▾ [Connection Status](#)

1 Item [Refresh](#) Show [ALL](#) ▾ Filter: Enable

|  | Details              | Session Manager | Type | Status | Connections | IP Address     | VLAN | Default Gateway | NIC Bonding | Entity Links (expected / actual) | Certificate Used |
|--|----------------------|-----------------|------|--------|-------------|----------------|------|-----------------|-------------|----------------------------------|------------------|
|  | <a href="#">Show</a> | SessionManager  | SM   | Up     | 18          | 10.64.41.42/24 | ---  | 10.64.41.1      | Disabled    | 12/12                            | SIP CA           |

Select : None

- Click a **Security Module** and select **Certificate Management** → **Update Installed Certificates**.



**AVAYA** Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Session Manager](#) ✕ [Inventory](#) ✕ [Home](#)

[Home](#) / [Elements](#) / [Session Manager](#) / [System Status](#) / [Security Module Status](#) - Security Module Status [Help ?](#)

### Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

[Reset](#) [Synchronize](#) [Certificate Management](#) ▾ [Connection Status](#)

1 Item [Refresh](#) Show [ALL](#) ▾ Filter: Enable

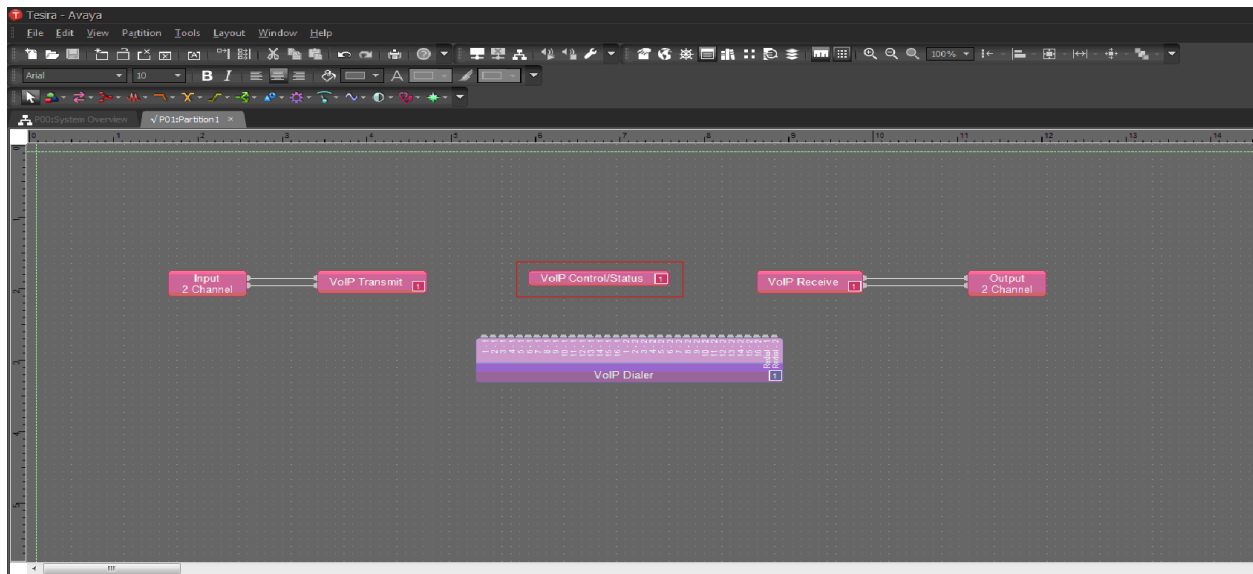
|  | Details              | Session Manager | Type | Status | Connections | IP Address     | VLAN | Default Gateway | NIC Bonding | Entity Links (expected / actual) | Certificate Used |
|--|----------------------|-----------------|------|--------|-------------|----------------|------|-----------------|-------------|----------------------------------|------------------|
|  | <a href="#">Show</a> | SessionManager  | SM   | Up     | 18          | 10.64.41.42/24 | ---  | 10.64.41.1      | Disabled    | 12/12                            | SIP CA           |

Select : None

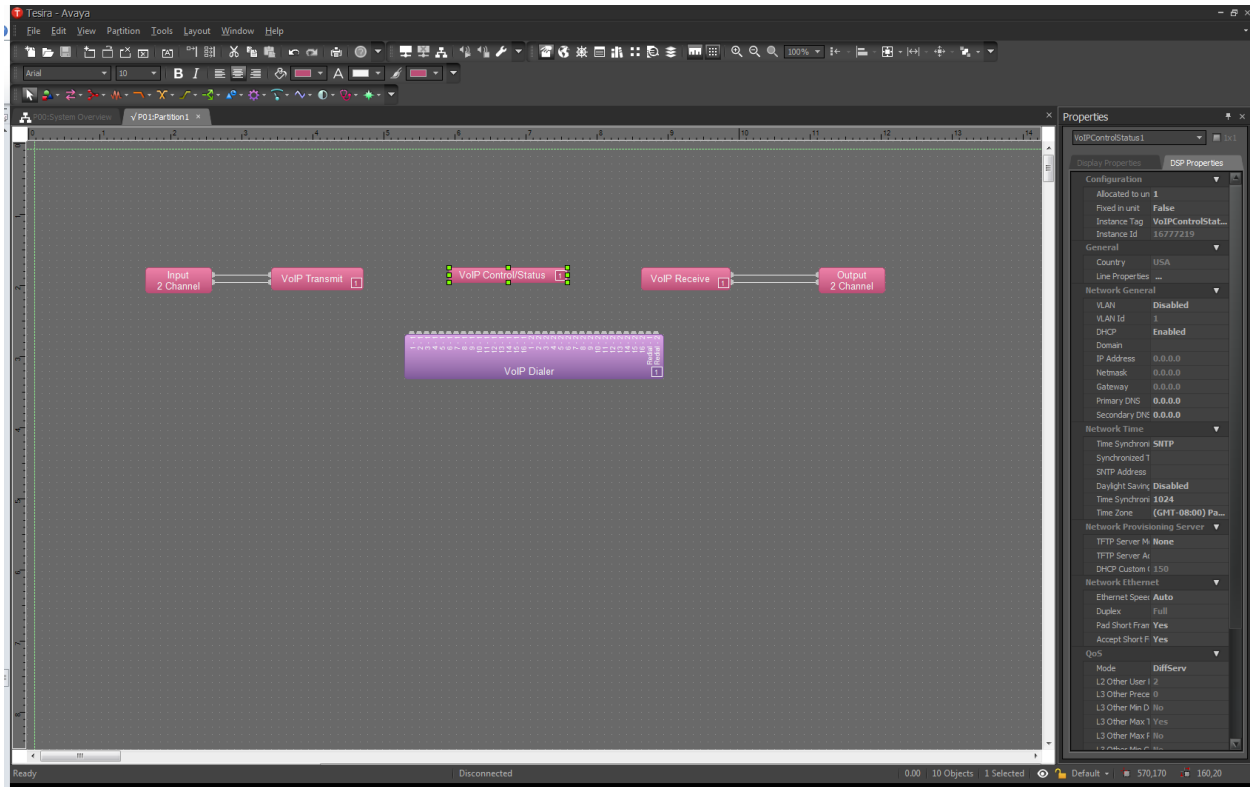
## 7. Configure Biamp Tesira SVC-2

Biamp installs, configures, and customizes the Tesira SVC-2 application for their end customers. This section only provides steps to configure Biamp Tesira SVC-2 to interface with Session Manager. Select the Tesira icon from Desktop to start Tesira software and design a VoIP system. How to configure a Tesira system is out of the scope.

- Highlight the **VoIPControl/Status** block, as shown below.



- Click right mouse button and select **Properties**, and the Properties menu will display on the right



- Navigate the **Protocol SIP→Transport** to configure transport to be used. The default is UDP. When TLS is selected, please refer to Tesira Operational Manual for additional configuration.



- Select **Line Properties** under the General section

The screenshot shows a 'Properties' dialog box for 'VoIPControlStatus1'. The 'General' section is expanded, and 'Line Properties' is highlighted with a red box. The 'Configuration' section shows 'Allocated to unit' as 1, 'Fixed in unit' as False, 'Instance Tag' as VoIPControlStatus1, and 'Instance Id' as 16777227. The 'Network General' section shows 'VLAN' as Disabled, 'VLAN Id' as 1, 'DHCP' as Enabled, 'Domain' as Disabled, 'IP Address' as Enabled, 'Netmask' as 255.255.255.0, 'Gateway' as 10.64.43.1, 'Primary DNS' as 205.171.3.65, and 'Secondary DNS' as 205.171.2.65. The 'Network Time' section shows 'Time Synchronizal' as SNTP, 'Synchronized Time' as empty, 'SNTP Address' as empty, 'Daylight Savings T' as Disabled, 'Time Synchronizal' as 1024, and 'Time Zone' as (GMT-08:00) Pacifi... The 'Network Provisioning Server' section shows 'TFTP Server Mode' as None, 'TFTP Server Addr' as 172.16.8.128, and 'DHCP Custom Op' as 150. The 'Network Ethernet' section shows 'Ethernet Speed' as Auto.

| Configuration     |                    |
|-------------------|--------------------|
| Allocated to unit | 1                  |
| Fixed in unit     | False              |
| Instance Tag      | VoIPControlStatus1 |
| Instance Id       | 16777227           |

| General         |     |
|-----------------|-----|
| Country         | USA |
| Line Properties | ... |

| Network General |               |
|-----------------|---------------|
| VLAN            | Disabled      |
| VLAN Id         | 1             |
| DHCP            | Enabled       |
| Domain          | Disabled      |
| IP Address      | Enabled       |
| Netmask         | 255.255.255.0 |
| Gateway         | 10.64.43.1    |
| Primary DNS     | 205.171.3.65  |
| Secondary DNS   | 205.171.2.65  |

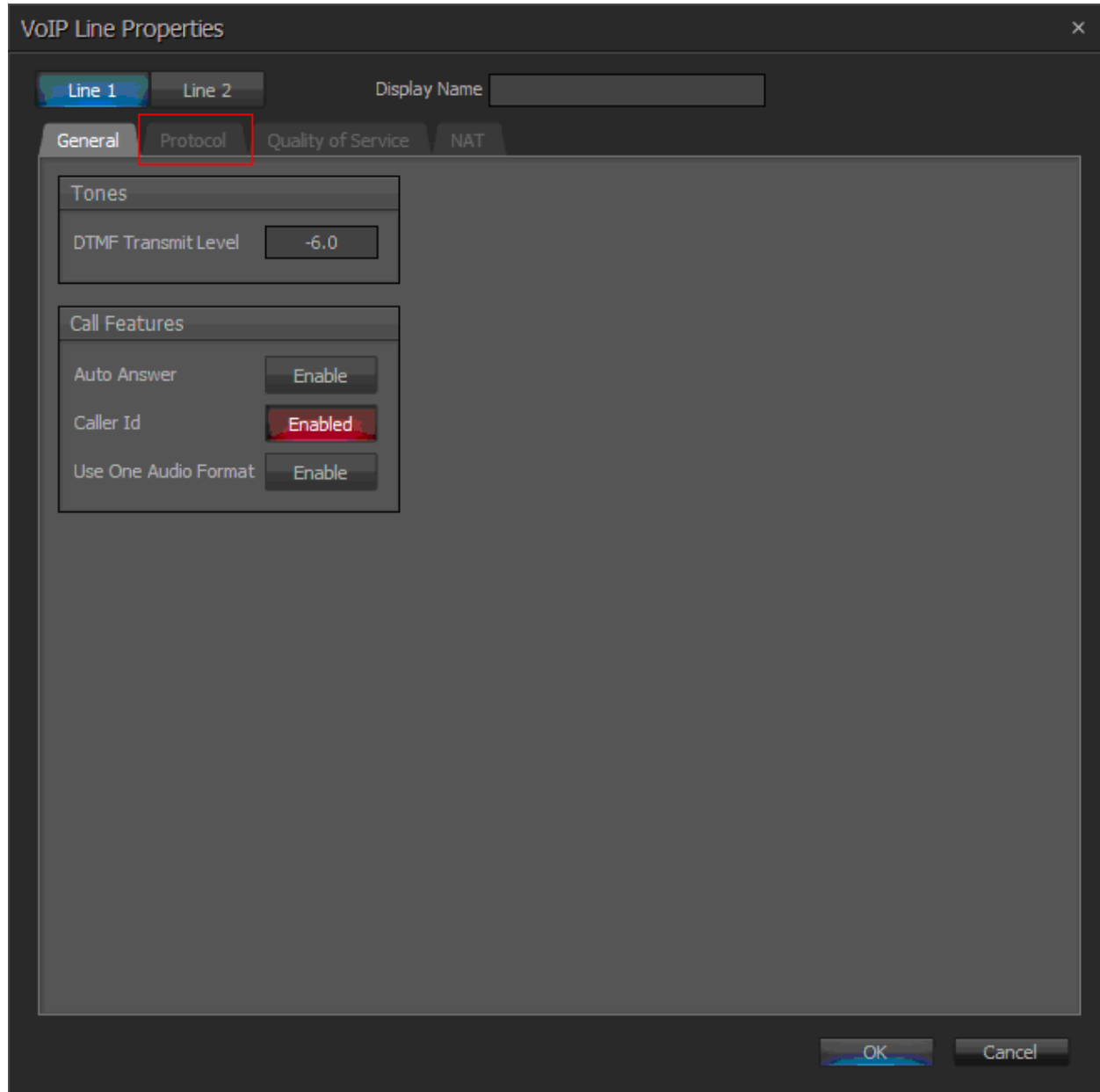
| Network Time       |                       |
|--------------------|-----------------------|
| Time Synchronizal  | SNTP                  |
| Synchronized Time  |                       |
| SNTP Address       |                       |
| Daylight Savings T | Disabled              |
| Time Synchronizal  | 1024                  |
| Time Zone          | (GMT-08:00) Pacifi... |

| Network Provisioning Server |              |
|-----------------------------|--------------|
| TFTP Server Mode            | None         |
| TFTP Server Addr            | 172.16.8.128 |
| DHCP Custom Op              | 150          |

| Network Ethernet |      |
|------------------|------|
| Ethernet Speed   | Auto |



- From the Line Properties page, click the **Protocol** tab.



- From the Protocol page, provide the following information:
  - **SIP User Name** – Enter a user created in **Section 6.11**.
  - **Authentication User Name** – Enter a user created in **Section 6.11**.
  - **Authentication Password** – Enter the password for the user in **Section 6.11**
  - **Proxy Vendor** – Select Avaya SM
  - **Proxy Address** – Enter the IP address of Session Manager.
  - **Proxy Port** – Enter either 5060 or 5061.
    - TLS – 5061
    - UDP or TCP – 5060
  - Click on the **OK** button. Default values may be used for all other fields.

Note: *Biamp Tesira SVC-2 can provide two inbound extensions (L1 and L2).*

**VoIP Line Properties**

Line 1 | Line 2 | Display Name

General | **Protocol** | Quality of Service | NAT

**SIP**

|                          |                                                                |                            |              |
|--------------------------|----------------------------------------------------------------|----------------------------|--------------|
| SIP User Name            | 72032                                                          | Registration Expiration    | 3600 seconds |
| SIP Display Name         | 72032,SM                                                       | Signaling Port             | 5060         |
| SIP Domain Name          |                                                                | T1 Timer                   | 500 ms       |
| Authentication User Name | 72032                                                          | Retransmit Timeout         | 32000 ms     |
| Authentication Password  | .....                                                          | Session Timer              | Enabled      |
| Proxy Vendor             | Avaya SM                                                       | Session Refresher          | Auto         |
| Proxy Address            | 10.64.41.42                                                    | Session Expiration         | 1800 seconds |
| Proxy Port               | 5060                                                           | Minimum Session Expiration | 90 seconds   |
| Outbound Proxy Address   |                                                                | Pack                       | None         |
| Outbound Proxy Port      | 5060                                                           |                            |              |
| Local Dial Plan          | [2-9]11 0T 011xxx.T [0-1][2-9]xxxxxxxx [2-9]xxxxxxxx [2-9]xxxT |                            |              |

**RTP/SRTP**

|                     |          |
|---------------------|----------|
| Port Start          | 10000    |
| Port End            | 14999    |
| Static RTP Port     | Enable   |
| SRTP                |          |
| G.723 Encoding Rate | 5.3 kbps |

**SIPS**

|         |  |
|---------|--|
| Keyword |  |
|---------|--|

OK Cancel

## 8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Biamp Tesira SVC-2 successfully registers with the Session Manager server by following the **Home → Elements → Session Manager → System Status → User Registrations**.
- Place calls to and from Biamp Tesira SVC-2 and verify that the calls are successfully established with two-way talk path.

## 9. Conclusion

Biamp Tesira SVC-2 was compliance tested with Communication Manager and Session Manager. Biamp Tesira SVC-2 functioned properly for feature and serviceability. During compliance testing, Biamp Tesira SVC-2 successfully registered with Session Manager, placed and received calls to and from SIP and non-SIP telephones, and executed other telephony features like source transfer.

## 10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

- [1] *Administering Avaya Aura™ Communication Manager*, Release 6.0, June 2010, Issue 6.0, Document Number 03-300509
- [2] *Administering Avaya Aura® Session Manager*, Release 6.1, November 2010, Issue 1.1, Document Number 03-603324
- [3] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010

The following document was provided by Biamp.

- [4] *Tesira Operation Manual*, Document.

---

**©2012 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](mailto:devconnect@avaya.com).