



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Cogito Dialog with Avaya Aura® Application Enablement Services Release 8.1 and Avaya Session Border Controller for Enterprise Release 8.1 Using TLS and SRTP - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cogito Dialog to interoperate with Avaya Aura® Application Enablement Services and Avaya Session Border Controller for Enterprise. Cogito Dialog is a SIPREC call recording and analysis solution.

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 configuration steps required for Cogito Dialog to interoperate with Avaya Aura® Application Enablement Services and Avaya Session Border Controller for Enterprise (Avaya SBCE). Cogito Dialog is a SIPREC call recording, analysis and a cloud-based solution.

In the compliance testing, Cogito Dialog used the Java Telephony API (JTAPI) client to access the Telephony Services Application Program Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor contact center agents on Avaya Aura® Communication Manager. The SIPREC call recording capabilities of the Avaya SBCE are used to capture the media associated with the monitored agents as they are on call with a PSTN customer through a SIP trunking.

2. General Test Approach and Test Results

The general test approach was to verify the features and serviceability of the Cogito Dialog successfully integrate with Application Enablement Services using JTAPI and utilize SIPREC in the Avaya SBCE for call recording.

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 this Application Note, the interface between Avaya systems and the Cogito recording server utilizes the secure SIP Transport Layer Security (TLS) and secure RTP.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of

the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

To verify the monitor events and call recording on the agent devices, the following features and functionalities were exercised during the compliance test.

- Verifying connection of Cogito JTAPI client to Application Enablement TSAPI services.
- Response to SIP OPTIONS queries.
- Caller ID Presentation.
- Call recording of inbound calls from SIP trunk to elite contact center queue and then available agent answers the calls.
- Call recording of inbound calls from SIP trunk directly to agent.
- Call recording of outbound calls from agents to SIP trunk.
- Call recording of inbound call from SIP trunk to SIP agent remote worker.
- Call recording of mute, hold and transfer calls on the agent endpoints.
- Load balancing using the round-robin method for multiple Cogito recording servers.
- Serviceability testing – The behavior of Cogito recording server under different failure conditions.

Note: A SIP Agent remote worker was tested as part of this solution. The configuration necessary to support the SIP remote worker is beyond the scope of these Application Notes and is not included in the document.

2.2. Test Results

The compliance test of the Cogito recording solution was completed successfully with the exception of the observations or limitations described below.

- Current design of Cogito Dialog only records SIP trunk calls from/to monitored agent endpoints. The SIP trunk calls from to regular endpoints were not recorded.
- Calls between an internal agent endpoint and a SIP agent remote worker endpoint were not recorded or not supported by Cogito.
- Cogito stops recording as the agent places a call on hold and creates a new recording as the agent resumes the call. Therefore there is no recording during the time that the agent holds the call.
- Cogito does not record a conference call between SIP trunk and two agents.
- An issue was encountered in the Cogito Dialog, where the audio direction was not shown correctly between agent and customer (PSTN user). Cogito was able to implement a fix that showed the proper audio direction on the dashboard.

2.3. Support

Technical support on Cogito Dialog can be obtained through the following:

- Phone: (617) 580-3101
- Email: avayasupport@cogitocorp.com

3. Reference Configuration

The **Figure 1** below illustrates the test configuration diagram for the compliance test. In the test diagram, the SIP trunk was configured in the Avaya SBCE to connect to service provider for calls from PSTN to enterprise and versa. The Cogito Dialog solution established a connection to Application Enablement TSAPI services using JTAPI client and receives SIP messages and audio call recording from the Avaya SBCE. For load balancing using the round-robin method, Cogito recommends 15 call recorders in configuration for scaling and redundancy, while 3 were used in this test.

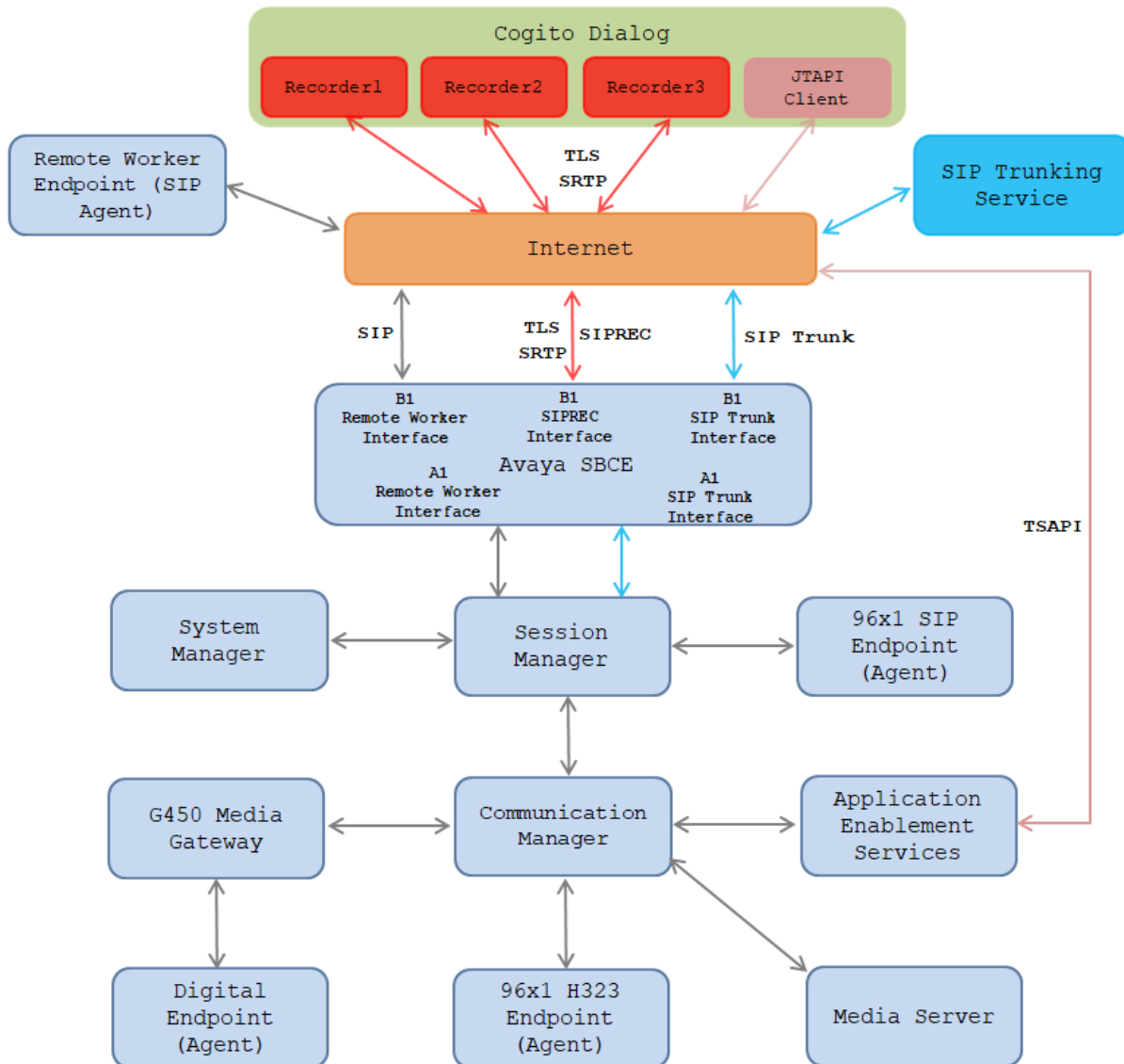


Figure 1 Test Configuration Diagram for Cogito Dialog

The following table indicates the IP addresses that were assigned to the systems in the test configuration diagram:

Description	IP Address
System Manager	10.33.1.10
Session Manager	10.33.1.11
Communication Manager	10.33.1.6
Application Enablement Services	10.33.1.14
Session Border Controller for Enterprise	10.33.10.100
Media Server	10.33.1.30
G450 Media Gateway	10.33.1.8
H.323 Endpoints	10.33.5.10-11
SIP Endpoints	10.33.5.12-14
Cogito Recording server 1	192.218.23.33
Cogito Recording server 2	192.217.121.209
Cogito Recording server 3	192.197.166.196
Cogito JTAPI Client	192.232.32.110

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtualized Environment	8.1.0.1.1 (01.0.890.0-25442)
Avaya Aura® System Manager running on Virtualized Environment	8.1.0.0 (8.1.0.0.810007)
Avaya Aura® Session Manager running on Virtualized Environment	8.1.0.0 Build No. 8.1.0.0.733078 Software Update Rev. No. 8.1.0.0.079814
Avaya Aura® Application Enablement Services	8.1.0
Avaya Session Border Controller for Enterprise	8.1.0.0-14-18490
Avaya Aura® Media Server running on Virtualized Environment	8.0.1.121_2019.04.29
Avaya G450 Media Gateway	41.16.0
Avaya 96x1 IP Deskphones	6.8202 (H.323) 7.1.6 (SIP)
Avaya 9408 Digital Deskphone	2.0 SP8 (R19)
Cogito Dialog	Kilmarnock 1.036
Cogito JTAPI Client	1.6.3

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager.

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	4 of	12
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n	
ARS?	y	Computer Telephony Adjunct Links?	y	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	n	DCS (Basic)?	y	
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y	

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page	1 of	3
CTI LINK				
CTI Link:	2			
Extension:	3331			
Type:	ADJ-IP			
				COR: 1
Name:	AES81			
Unicode Name?	n			

5.3. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                                     Page 5 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                      Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                Switch Name:
      Emergency Extension Forwarding (min): 10
      Enable Inter-Gateway Alternate Routing? n
      Enable Dial Plan Transparency in Survivable Mode? n
                                COR to Use for DPT: station
      EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
      Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
      Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
      Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
      Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
      Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
      Copy UCID for Station Conference/Transfer? y
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to ASAI and it will be used by the TJAPI application.

```
change system-parameters features                                     Page 13 of 20
                                FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
      Callr-info Display Timer (sec): 10
                                Clear Callr-info: next-call
      Allow Ringer-off with Auto-Answer? n

      Reporting for PC Non-Predictive Calls? n

      Agent/Caller Disconnect Tones? n
      Interruptible Aux Notification Timer (sec): 3
      Zip Tone Burst for Callmaster Endpoints: double

ASAI
      Copy ASAI UII During Conference/Transfer? y
      Call Classification After Answer Supervision? y
                                Send UCID to ASAI? y
      For ASAI Send DTMF Tone to Call Originator? y
      Send Connect Event to ASAI For Announcement Answer? n
      Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```


5.4. Administer AE Services

To administer the transport link to AES, use the command “change ip-services”. On Page 1, add an entry with the following values. Service Type should be selected as **AESVCS**, enter “y” in the **Enabled**, “procr” in the **Local Node** and 8765 in the **Local Port**.

change ip-services					Page	1 of
4						
IP SERVICES						
Service	Enabled	Local	Local	Remote	Remote	
Type		Node	Port	Node	Port	
AESVCS	y	procr	8765			

Go to **Page 4**, enter the following values. **AE Services Server** should be the AES host name, enter a password in the **Password** field and select “y” in the **Enabled** field.

Note: The password entered for **Password** field must match the password on the AES server in the Switch Connection in **Section 6.3**. The **AE Services Server** should match the host name of the AES server. To obtain the host name of AES server, use the command “**uname -n**” in the AES server Linux command prompt.

change ip-services				Page	4 of
4					
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	aes8	*	y	in use	
2:	aes81	*	y	in use	

5.5. Administer Hunt Group

This section provides the Hunt Group configuration for the call center agents. Agents will log into the Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.8**.

add hunt-group 1		Page 1 of 4
HUNT GROUP		
Group Number: 1	ACD? y	
Group Name: Skill-1	Queue? y	
Group Extension: 3320	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	
SIP URI:		

On **Page 2** of the Hunt Group form, enable the **Skill** option and **Both** in the **Measured** field.

add hunt-group 1		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in	
20		
Measured: both		
Supervisor Extension:		
Controlling Adjunct: none		
VuStats Objective:		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

5.6. Administer Vector

Use the command “change vector n” while “n” is the vector number from 1-8000. The example of the vector 1 with a basic scripting is shown below. Vector 1 is used for the configuration of the VDN in the next step.

```
change vector 1                                     Page 1 of 6
6
                                CALL VECTOR

      Number: 1                                Name: Contact Center
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock?
n
      Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing?
y
  Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
  Variables? y      3.0 Enhanced? y
01 wait-time      10 secs hearing 1100      then silence
02 queue-to      skill 1      pri m
03 wait-time      5 secs hearing ringback
04 check      skill 1      pri m if expected-wait      < 30
05 announcement 1104
06 queue-to      skill 1      pri m
07 stop
```

5.7. Administer VDN

Use the “add vdn <ext>” command to add a VDN number. In the **Destination** field, enter **Vector Number 1** as configured in **Section 5.6** above and keep other fields at their default values.

```
add vdn 3340                                     Page 1 of 3
3
                                VECTOR DIRECTORY NUMBER

                                Extension: 3340
                                Name*: Contact Center 1
                                Destination: Vector Number 1
                                Attendant Vectoring? n
                                Meet-me Conferencing? n
                                Allow VDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: both      Report Adjunct Calls as
ACD*? n
      Acceptable Service Level (sec): 20
      VDN of Origin Annc. Extension*:
                                1st Skill*:
                                2nd Skill*:
                                3rd Skill*:
```

5.8. Administer Agent Login ID

To add an **Agent LoginID**, use the command “add agent-loginID <agent ID>” for each agent. In the compliance test, three agent login IDs (1000, 1001, and 1002) were created.

add agent-loginID 1000		Page 1 of 2
AGENT LOGINID		
Login ID: 1000		AAS? n
Name: Agent 1000		AUDIX? n
TN: 1		
COR: 1		
Coverage Path:		LWC Reception: spe
Security Code: 1234		LWC Log External Calls? n
Attribute:		AUDIX Name for Messaging:
		LoginID for ISDN/SIP Display? n
		Password:
		Password (enter again):
		Auto Answer:
station		
		MIA Across Skills: system
AUX Agent Considered Idle (MIA)? system	ACW Agent Considered Idle: system	
	Aux Work Reason Code Type: system	
	Logout Reason Code Type: system	
	Maximum time agent in ACW before logout (sec): system	
	Forced Agent Logout Time: :	
WARNING: Agent must log in again before changes take effect		

On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.

add agent-loginID 1000		Page 2 of 2	
AGENT LOGINID			
Direct Agent Skill:		Service Objective? n	
Call Handling Preference: skill-level		Local Call Preference? n	
SN	RL SL	SN	RL SL
1: 1	1	16:	
2:		17:	
3:		18:	
4:		19:	
5:		20:	
6:			
7:			
8:			
9:			
10:			
11:			
12:			
13:			
14:			
15:			

5.9. Configure SIP Trunk

Use the command “change trunk-group n” where “n” is number of the trunk group that is previously configured to connect to Avaya SBCE. Go to **Page 3**, select “*shared*” in the **UI Treatment** field. With the selection of shared UI, the **Send UCID** field is present and select “y” in this field.

change trunk-group 3	Page 3 of 5
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n Numbering Format: private	
	UI Treatment: shared
	Maximum Size of UI Contents: 128
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Send UCID? y	
Show ANSWERED BY on Display? y	

On **Page 4**, enter the value “1” in the **Universal Call ID (UCID)** field and keep other fields at default values.

change trunk-group 3	Page 4 of 5
SHARED UI FEATURE PRIORITIES	
ASAI:	
Universal Call ID (UCID): 1	
MULTI SITE ROUTING (MSR)	
In-VDN Time: 3	
VDN Name: 4	
Collected Digits: 5	
Other LAI Information: 6	
Held Call UCID: 7	
ECD UI: 8	

6. Configure Avaya Aura® Application Enablement Services


This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch AE web interface
- Verify license
- Administer Switch Connection
- Administer TSAPI link
- Administer CTI user
- Administer Security Database
- Administer ports
- Restart services

6.1. Launch AE web Interface


Access the AE web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page below the header. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a label "Username" and a text input field. Below the input field is a "Continue" button. Another thick red horizontal bar is located at the bottom of the page, just above the footer text.

The **Welcome to OAM** screen is displayed next.

 **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Tue Aug 27 21:15:41 2019 from 10.33.100.9
Number of prior failed login attempts: 0
HostName/IP: aes81/10.207.80.111
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.0.0.9-1
Server Date and Time: Thu Aug 29 14:40:08 IST 2019
HA Status: Not Configured

HomeHome | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).

LicensingHome | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▼ Licensing
 - WebLM Server Address
 - WebLM Server Access
 - Reserved Licenses
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

Select **Licensed products** → **APPL_ENAB** → **Application Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left pane displays a tree view with 'L...' expanded, showing various components like ASBCE, Session_Border_Controller_E_AE, CCTR, CE, COMMUNICATION_MANAGER, and SYSTEM_MANAGER. The right pane displays the 'Licensed Features' table, which lists 13 items. The table has three columns: 'Feature (License Keyword)', 'Expiration date', and 'Licensed capacity'. The 'TSAPI Simultaneous Users' feature is highlighted, showing a permanent expiration date and a licensed capacity of 500.

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	500
AES HA LARGE VALUE_AES_HA_LARGE	permanent	500
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	500
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	500
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	500
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	500
DLG VALUE_AES_DLG	permanent	500
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	500
CVLAN Proprietary Links	permanent	500

6.3. Administer Switch Connection

Select **Communication Manager Interface** → **Switch Connections** from the left pane of the **Management Console**, enter a name in the **Switch Connection** box and click the **Add** button (not shown). Enter the password as configured in **Section 5.4** in the **Switch Password** and **Confirm Switch Password**, and check on **Processor Ethernet** field if the Processor Ethernet is used in Communication Manager. Click the **Apply** button to save the configuration.

The screenshot shows the 'Communication Manager Interface | Switch Connections' page. On the left is a navigation pane with 'Communication Manager Interface' expanded and 'Switch Connections' selected. The main area displays the 'Connection Details - interopcm' form. The form includes fields for 'Switch Password' and 'Confirm Switch Password' (both masked with dots), a 'Msg Period' of 30 minutes, and checkboxes for 'Provide AE Services certificate to switch' (checked), 'Secure H323 Connection' (unchecked), and 'Processor Ethernet' (checked). 'Apply' and 'Cancel' buttons are at the bottom.

Select the **interopcm** switch connection has been added above and selects **Edit PE/CLAN IPs** to add the IP address of the switch connection.

The screenshot shows the 'Communication Manager Interface | Switch Connections' page. On the left is the same navigation pane. The main area displays the 'Switch Connections' section with an 'Add Connection' button and a table. The table has columns: 'Connection Name', 'Processor Ethernet', 'Msg Period', and 'Number of Active Connections'. One connection, 'interopcm', is listed with 'Processor Ethernet' set to 'Yes', 'Msg Period' of 30, and 'Number of Active Connections' of 1. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
interopcm	Yes	30	1

Enter the IP address of the Processor Ethernet of Communication Manager in the box and click the **Add/Edit Name of IP** button to add the IP.

The screenshot shows the 'Communication Manager Interface' with a red header bar containing 'Switch Connections' and links for 'Home | Help | Logout'. A left sidebar lists various services, with 'Communication Manager Interface' expanded to show 'Switch Connections'. The main content area is titled 'Edit Processor Ethernet IP - interopcm'. It features a text input field containing '10.33.1.6' and an 'Add/Edit Name or IP' button. Below this is a table with two columns: 'Name or IP Address' and 'Status'. The table contains one entry with '10.33.1.6' and 'In Use'. A 'Back' button is located at the bottom left of the main content area.

Name or IP Address	Status
10.33.1.6	In Use

Select the **Edit H.323 Gatekeeper** button to add an IP address of gate keeper, the Gatekeeper IP address in this case is also the Processor Ethernet.

The screenshot shows the 'Communication Manager Interface' with a red header bar containing 'Switch Connections' and links for 'Home | Help | Logout'. A left sidebar lists various services, with 'Communication Manager Interface' expanded to show 'Switch Connections'. The main content area is titled 'Edit H.323 Gatekeeper - interopcm'. It features a text input field and an 'Add Name or IP' button. Below this is a section labeled 'Name or IP Address' with a radio button selected next to '10.33.1.6'. At the bottom, there are 'Delete IP' and 'Back' buttons.

6.4. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the 'TSAPI Links' management screen. On the left is a navigation pane with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded to show 'TSAPI Links' and 'TSAPI Properties'), 'TWS', 'Communication Manager Interface', 'High Availability', and 'Licensing'. The main area is titled 'TSAPI Links' and contains a table with columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

The **Add TSAPI Links** screen is displayed in the right side. The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “**interopcm**” which is added in the step above. For **Switch CTI Link Number**, select the CTI link number 2 from **Section 5.2**, select **Both** in the **Security** dropdown menu to support both unencrypted and encrypted TSAPI link. Retain the default values in the remaining fields.

The screenshot shows the 'Add TSAPI Links' configuration screen. The left navigation pane is the same as in the previous screenshot. The main area is titled 'Add TSAPI Links' and contains the following fields and buttons:

- Link**: A text input field containing the value '2'.
- Switch Connection**: A dropdown menu with 'interopcm' selected.
- Switch CTI Link Number**: A dropdown menu with '2' selected.
- ASAI Link Version**: A dropdown menu with '8' selected.
- Security**: A dropdown menu with 'Both' selected.
- Buttons**: 'Apply Changes' and 'Cancel Changes'.

6.5. Administer CTI User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane. Enter the desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

cogito

* Common Name

cogito

* Surname

cogito

* User Password

.....

* Confirm Password

.....

Admin Note

Avaya Role

None

Business Category

Car License

CM Home

Css Home

CT User

Yes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

Home Phone

Home Postal Address

Initials

Labeled URI

Mail

MM Home

Mobile

Organization

Pager

Preferred Language

English

Room Number

Telephone Number

Apply

Cancel

6.6. Configure Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Leave it as default as checked on **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services**.

The screenshot shows the 'Security | Security Database | Control' page. The left navigation pane lists various services, with 'Security' expanded to show 'Security Database' and 'Control'. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two checkboxes: 'Enable SDB for DMCC Service' (unchecked) and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services' (checked). An 'Apply Changes' button is located below the checkboxes.

Select **Security** → **Security Database** → **CTI Users** → **List All Users** and select the “cogito” CTI user which is created in **Section 6.5** and select **Edit** button (not shown). In the **Edit CTI User**, select the check box **Unrestricted Access** and click **Apply Changes** to save the configuration.

The screenshot shows the 'Security | Security Database | CTI Users | List All Users' page. The left navigation pane is the same as the previous screenshot, with 'Security Database' expanded to show 'CTI Users'. The main content area is titled 'Edit CTI User'. It displays the configuration for the 'cogito' user profile. The 'User Profile' section shows 'User ID' as 'cogito', 'Common Name' as 'cogito', 'Worktop Name' as 'NONE', and 'Unrestricted Access' as checked. The 'Call and Device Control' section shows 'Call Origination/Termination and Device Status' as 'None'. The 'Call and Device Monitoring' section shows 'Device Monitoring' as 'None', 'Calls On A Device Monitoring' as 'None', and 'Call Monitoring' as unchecked. The 'Routing Control' section shows 'Allow Routing on Listed Devices' as 'None'. At the bottom, there are 'Apply Changes' and 'Cancel Changes' buttons.

6.7. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane. In the **TSAPI Ports** section, select the radio button for **TSAPI Service Port 450** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

Networking | PortsHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ **Networking**

▶ AE Service IP (Local IP)

▶ Network Configure

Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

H.323 Ports

TCP Port Min20000

TCP Port Max29999

Local UDP Port Min20000

Local UDP Port Max29999

Server Media

RTP Local UDP Port Min*30000

RTP Local UDP Port Max*49999

* Note: The number of RTP ports needs to be double the number of extensions using server media.

SMS Proxy Ports

Proxy Port Min4101

Proxy Port Max4116

Apply ChangesRestore Defaults

KP; Reviewed:
SPOC 5/13/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

22 of 58
Cogito-SBCE81

6.8. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Click **Restart AE Server**.

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

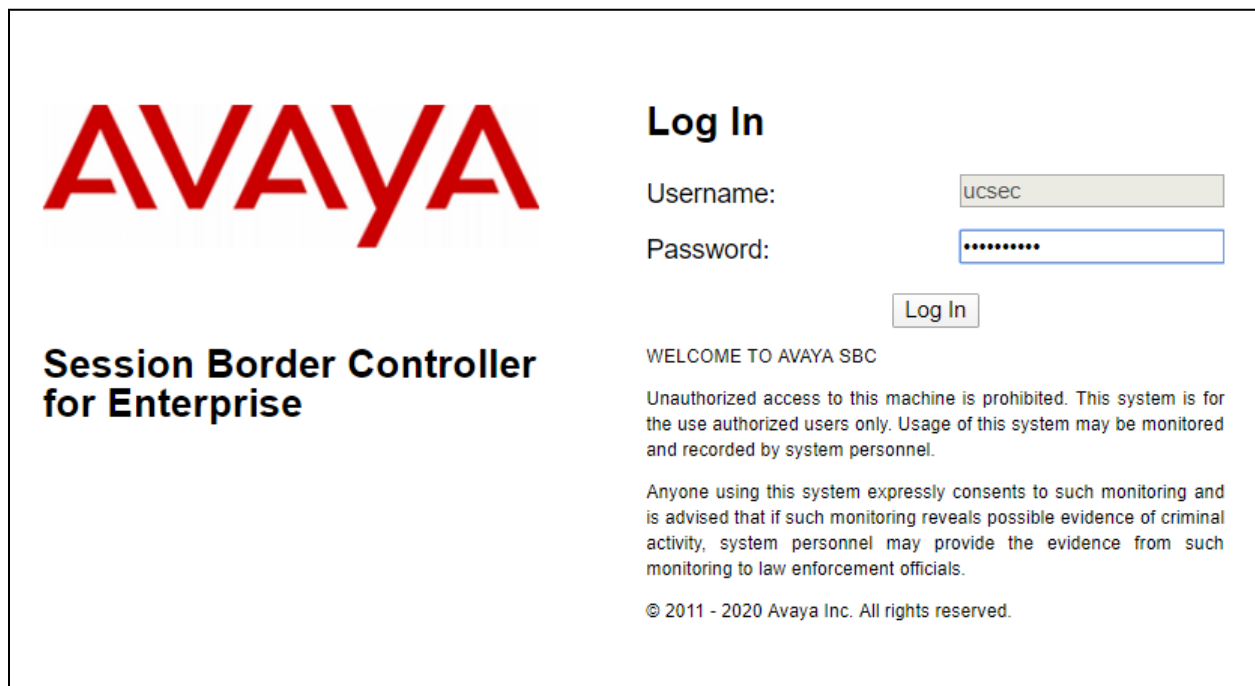
7. Configure Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE has been completed including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (e.g., A1 and B1).

On all screens described in this section, it is assumed that parameters are left at their default values unless specified otherwise.

7.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with appropriate credentials.

The image shows the Avaya Session Border Controller for Enterprise (SBCE) login page. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold black. On the right, under the heading 'Log In', there are input fields for 'Username:' (containing 'ucsec') and 'Password:' (containing seven dots). Below these fields is a 'Log In' button. Further down, there is a 'WELCOME TO AVAYA SBC' message, a disclaimer about unauthorized access, a consent statement, and a copyright notice for 2011-2020 Avaya Inc.

After logging in, the Dashboard screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

Session Border Controller for Enterprise

EMS Dashboard

- Device Management
 - System Administration
 - Backup/Restore
 - Monitoring & Logging

Dashboard

GUI DEBUG level log messages are currently enabled on one or more components. Leaving this log level enabled for extended periods of time is not recommended but will not have any adverse effects.

Information	
System Time	09:50:27 AM MDT Refresh
Version	8.1.0.0-14-18490
GUI Version	8.1.0.0-18490
Build Date	Mon Feb 03 17:23:09 UTC 2020
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	04/01/2020 09:13:44 MDT
Failed Login Attempts	0

Installed Devices

- EMS
- SBCE100

Active Alarms (past 24 hours)

Incidents (past 24 hours)

7.2. Verify Network Configuration and Enable Interfaces

To view the network information provided during installation, navigate to **Device Management**. In the right pane, click **View**.

Session Border Controller for Enterprise

Device Management

EMS Dashboard

- Device Management**
 - System Administration
 - Backup/Restore
 - Monitoring & Logging

Devices | Updates | SSL VPN | Licensing | Key Bundles

Device Name	Management IP	Version	Status						
SBCE100	10.33.10.100	8.1.0.0-14-18490	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

A System Information page will appear showing the information provided during installation. The **Appliance Name** field is the name of the device (**SBCE100**). This name will be referenced in other configuration screens. Interface **A1** and **B1** represent the private and public interfaces of the Avaya SBCE respectively. Each of these interfaces must be enabled after installation.

System Information: SBCE100

General Configuration

Appliance Name SBCE100
Box Type SIP
Deployment Mode Proxy

Device Configuration

HA Mode No
Two Bypass Mode No

License Allocation

Standard Sessions 512
Requested: 512
Advanced Sessions 512
Requested: 512
Scopia Video Sessions 512
Requested: 512
CES Sessions 512
Requested: 512
Transcoding Sessions 512
Requested: 512
CLID ---
Encryption Available: Yes ☒

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.33.1.51	10.33.1.51	255.255.255.0	10.33.1.1	A1
10.33.1.52	10.33.1.52	255.255.255.0	10.33.1.1	A1
10.33.1.53	10.33.1.53	255.255.255.0	10.33.1.1	A1
10.207.80.107	10.207.80.107	255.255.255.128	10.207.80.1	B1
10.207.80.108	10.207.80.108	255.255.255.128	10.207.80.1	B1
10.207.80.109	10.207.80.109	255.255.255.128	10.207.80.1	B1

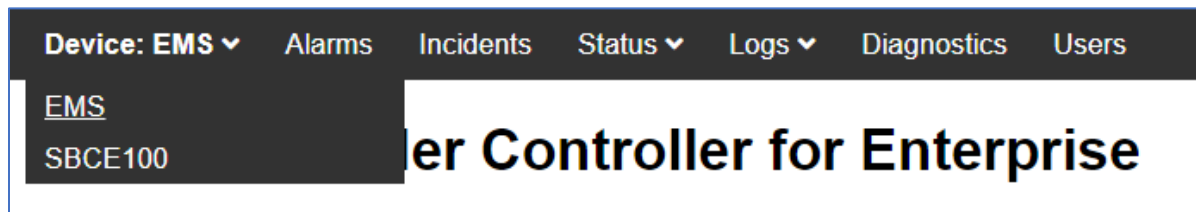
DNS Configuration

Primary DNS 10.33.100.60
Secondary DNS 8.8.8.8
DNS Location DMZ
DNS Client IP 10.33.1.51

Management IP(s)

IP #1 (IPv4) 10.33.10.100

From the right top corner of the window, select **Device** dropdown menu and select the SBCE system, e.g. **SBCE100**, the administration is displayed in the right pane.



To enable the interfaces, first navigate to **Network & Flows** → **Network Management** in the left pane. In the right pane, click on the **Interfaces** tab. Verify the **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the status **Enabled/Disabled** to toggle the state of the interface.

Device: SBCE100 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

Network Management

Interfaces Networks

Add VLAN

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

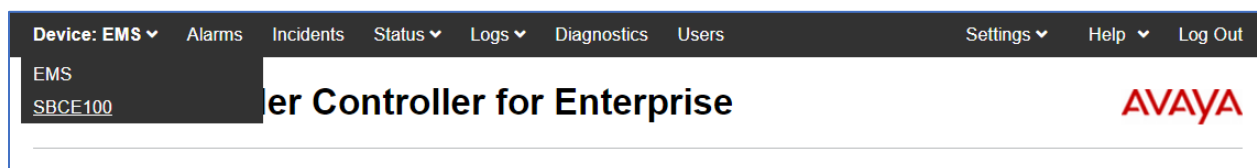
7.3. TLS Management

Note – Testing was done with System Manager signed identity certificates for Cogito recording server and Avaya SBCE. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between Session Manager and Avaya SBCE and between Avaya SBCE and Cogito recording server. The following procedures show how to create the client and server profiles.

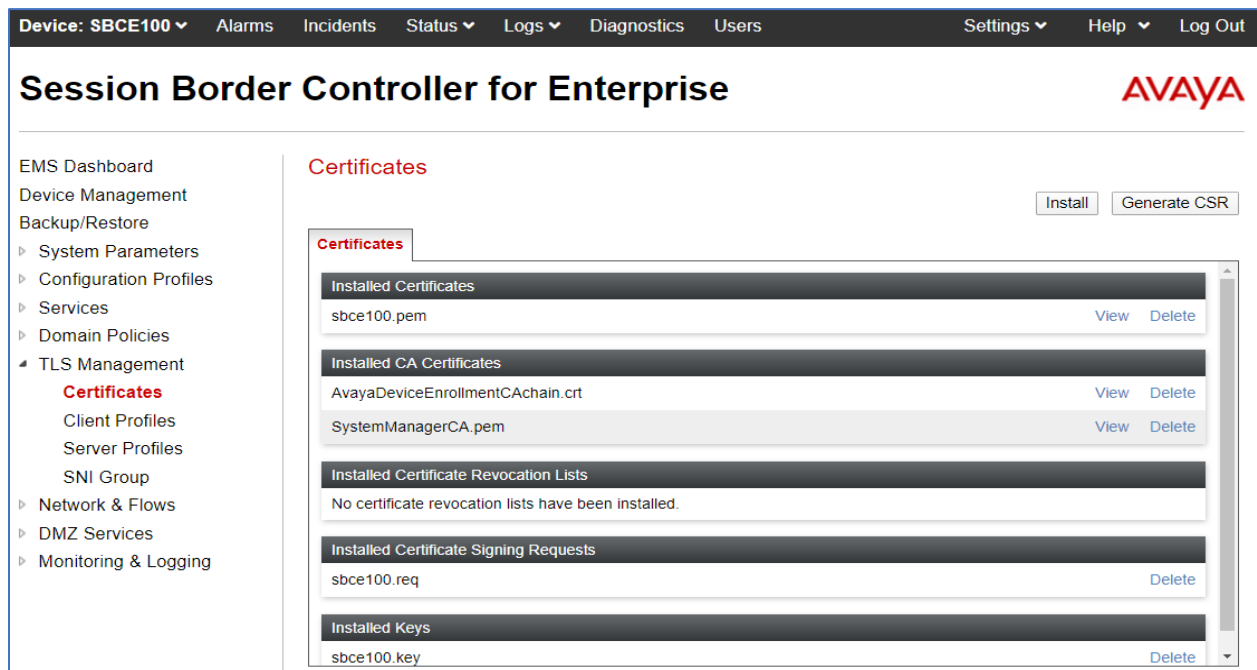
7.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

To access the SBCE configuration menus, select the SBCE device from the top navigation menu.



Step 1 - Select **TLS Management** → **Certificates** from the left-hand menu. Verify the following:

- System Manager CA certificate is present in the **Installed CA Certificates** area.
- System Manager CA signed identity certificate is present in the **Installed Certificates** area.
- Private key associated with the identity certificate is present in the **Installed Keys** area.



7.3.2. Server Profiles

Step 1 - Select **TLS Management** → **Server Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter a descriptive name. (e.g., **TLS_Server_Profile**).
- **Certificate:** select the identity certificate, e.g., **sbce100.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile	
Profile Name	<input type="text" value="TLS_Server_Profile"/>
Certificate	<input type="text" value="sbce100.pem"/>
SNI Options	<input type="text" value="None"/>
SNI Group	<input type="text" value="None"/>

Certificate Verification	
Peer Verification	<input type="text" value="None"/>
Peer Certificate Authorities	<div>AvayaDeviceEnrollmentCAchain.crt SystemManagerCA.pem</div>
Peer Certificate Revocation Lists	<div></div>
Verification Depth	<input type="text" value="0"/>

Next

The following screen shows the completed TLS Server Profile form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE100, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left sidebar contains a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates, Client Profiles, Server Profiles (highlighted), SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled "Server Profiles: TLS_Server_Profile" and features an "Add" button and a "Delete" button. Below this is a "Server Profiles" list with "TLS_Server_..." selected. The main configuration panel for the selected profile includes a description field and several sections:

- TLS Profile**
 - Profile Name: TLS_Server_Profile
 - Certificate: sbce100.pem
 - SNI Options: None
- Certificate Verification**
 - Peer Verification: None
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2, ☐ TLS 1.1, ☐ TLS 1.0
 - Ciphers: ☒ Default, ☐ FIPS, ☐ Custom
 - Value: HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

An "Edit" button is located at the bottom of the configuration panel.

7.3.3. Client Profiles

Step 1 - Select **TLS Management** → **Server Profiles**, and click on **Add**. Enter the following:

- **Profile Name:** enter a descriptive name (e.g., **TLS_Client_Profile**)
- **Certificate:** select the identity certificate, e.g., **sbce100.pem**, from pull down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **SystemManagerCA.pem**.
- Enter 1 under **Verification Depth**. Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile	
Profile Name	<input type="text" value="TLS_Client_Profile"/>
Certificate	<input type="text" value="sbce100.pem"/>
SNI	<input type="checkbox"/> Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	<input type="text" value="AvayaDeviceEnrollmentCAchain.crt"/> <input type="text" value="SystemManagerCA.pem"/>
Peer Certificate Revocation Lists	<input type="text"/>
Verification Depth	<input type="text" value="1"/>
Extended Hostname Verification	<input type="checkbox"/>
Server Hostname	<input type="text"/>

Next

The following screen shows the completed TLS **Client Profile** form:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE100, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various management options, with 'Client Profiles' highlighted under the 'TLS Management' section. The main content area is titled 'Client Profiles: TLS_Client_Profile' and features an 'Add' button and a 'Delete' button. Below this, there is a tabbed interface with the 'Client Profile' tab selected. The configuration form is divided into several sections: 'TLS Profile' (containing Profile Name, Certificate, and SNI), 'Certificate Verification' (containing Peer Verification, Peer Certificate Authorities, Peer Certificate Revocation Lists, Verification Depth, and Extended Hostname Verification), 'Renegotiation Parameters' (containing Renegotiation Time and Renegotiation Byte Count), and 'Handshake Options' (containing Version, Ciphers, and Value). The 'Edit' button is located at the bottom right of the form.

Device: SBCE100 Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Certificates
Client Profiles
Server Profiles
SNI Group
Network & Flows
DMZ Services
Monitoring & Logging

Client Profiles: TLS_Client_Profile

Add Delete

Client Profiles Click here to add a description.

Client Profile

TLS Profile	
Profile Name	TLS_Client_Profile
Certificate	sbce100.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

7.4. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Network & Flows → Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**SBCE100**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by one or more pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

- **Name:** enter a descriptive name.
- For the internal interface, set the **IP Address** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **IP Address** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port Avaya SBCE will listen on for each transport protocol. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061. For the external interface, the Avaya SBCE was configured to listen for TLS on port 5061.
- **TLS Profile:** select the server TLS profile in the dropdown menu.

The screenshot shows a configuration window titled "Edit Signaling Interface" with a close button (X) in the top right corner. The window contains several input fields and a checkbox, organized in a light gray bordered box. The fields are as follows:

Name	Public_SIPREC_Sig
IP Address	Public_B1 (B1, VLAN 0) 10.207.80.109
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	5061
TLS Profile	TLS_Server_Profile
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

At the bottom center of the configuration box is a "Finish" button.

For the testing, the list of signaling interfaces in the table below created:

Name	IP address	Description
Private1_Sig	10.33.1.51	The private signaling interface connects to Session Manager
Public1_Sig	10.50.207.107	The public signaling interface connects to Service Provider
Private_Sig_RW	10.33.1.52	The private signaling interface for SIP remote worker connects to Session Manager
Public_Sig_RW	10.50.207.108	The public signaling interface for SIP remote worker connects to SIP remote worker endpoint
Private_SIPREC_Sig	10.33.1.53	This interface is not used during the testing since Cogito recording server resides in the public network.
Public_SIPREC_Sig	10.50.207.109	The public signaling interface connects to Cogito recording server

The screenshot below show the list of signaling interfaces used during the compliance test.

Device: SBCE100
Alarms
Incidents
Status
Logs
Diagnostics
Users
Settings
Help
Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
Advanced Options
DMZ Services
Monitoring & Logging

Signaling Interface

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_Sig_RW	10.33.1.52 Private_A1 (A1, VLAN 0)	5060	5060	5061	TLS_Server_Profile	Edit Delete
Private1_Sig	10.33.1.51 Private_A1 (A1, VLAN 0)	5060	5060	5061	TLS_Server_Profile	Edit Delete
Public1_Sig	10.207.80.107 Public_B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
Public_Sig_RW	10.207.80.108 Public_B1 (B1, VLAN 0)	5060	5060	5061	TLS_Server_Profile	Edit Delete
Private_SIPREC_Sig	10.33.1.53 Private_A1 (A1, VLAN 0)	5060	5060	5061	TLS_Server_Profile	Edit Delete
Private2_Sig	10.33.1.54 Private_A1 (A1, VLAN 0)	5060	5060	5061	TLS_Server_Profile	Edit Delete
Public2_Sig	10.207.80.90 Public_B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
Public_SIPREC_Sig	10.207.80.109 Public_B1 (B1, VLAN 0)	5060	5060	5061	TLS_Server_Profile	Edit Delete

7.5. Media Interface

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Network & Flows → Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**SBCE100**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by one or more pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

- **Name:** enter a descriptive name.
- For the internal media interface, set the **IP Address** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **IP Address** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far-end. For the testing, the default port range was used for the SIPREC public media interface.

The screenshot shows a dialog box titled "Edit Media Interface" with a close button (X) in the top right corner. The dialog contains three main sections for configuration:

- Name:** A text input field containing "Public_SIPREC_Med".
- IP Address:** A dropdown menu showing "Public_B1 (B1, VLAN 0)" with a downward arrow. Below it is a text input field containing "10.207.80.109".
- Port Range:** Two text input fields, the first containing "35000" and the second containing "40000", separated by a hyphen.

At the bottom center of the dialog is a button labeled "Finish".

For the testing, list of media interfaces were added and shown in the table below.

Name	IP address	Description
Private1_Med	10.33.1.51	The private media interface connects to enterprise endpoints such as media gateway and agent endpoints
Public1_Med	10.207.80.107	The public media interface connects to media gateway of Service Provider
Private_Med_RW	10.33.1.52	The private media interface for SIP remote worker connects to enterprise endpoints
Public_Med_RW	10.207.80.108	The public media interface for SIP remote worker connects to SIP remote worker endpoint
Private_SIPREC_Med	10.33.1.53	The private media interface for SIPREC is not used for this testing
Public_SIPREC_Med	10.207.80.109	The public media interface for SIPREC sends media to Cogito SIP recording server

The screenshot below shows the list of media interface used for the testing.

Device: SBCE100
Alarms
Incidents
Status
Logs
Diagnostics
Users
Settings
Help
Log Out

Session Border Controller for Enterprise

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
Advanced Options
DMZ Services
Monitoring & Logging

Media Interface

Name	Media IP Network	Port Range	
Private1_Med	10.33.1.51 Private_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Public1_Med	10.207.80.107 Public_B1 (B1, VLAN 0)	35000 - 40000	Edit Delete
Private_SIPREC_Med	10.33.1.53 Private_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Private_Med_RW	10.33.1.52 Private_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Public_Med_RW	10.207.80.108 Public_B1 (B1, VLAN 0)	35000 - 40000	Edit Delete
Private2_Med	10.33.1.54 Private_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Public2_Med	10.207.80.90 Public_B1 (B1, VLAN 0)	35000 - 40000	Edit Delete
Public_SIPREC_Med	10.207.80.109 Public_B1 (B1, VLAN 0)	10000 - 40000	Edit Delete

KP; Reviewed:
SPOC 5/13/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

36 of 58
Cogito-SBCE81

7.6. Server Configuration

A server configuration profile defines the attributes of the physical server. To create a new profile, navigate to **Services** → **SIP Servers** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by one or more pop-up windows in which the profile parameters can be configured

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE100, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. The left sidebar contains a menu with categories like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, and Services. Under Services, SIP Servers is selected, showing a list of profiles: IPO, SM, Recorder2, SP1, Recorder1 (highlighted), and SP2. The main content area is titled "SIP Servers: Recorder1" and includes an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this is a tabbed interface with "General", "Heartbeat", "Registration", "Ping", and "Advanced" tabs. The "General" tab is active, showing fields for Server Type (Recording Server), TLS Client Profile (TLS_Client_Profile), and DNS Query Type (NONE/A). A table lists the IP Address / FQDN (192.218.23.33), Port (5061), and Transport (TLS). An "Edit" button is located at the bottom right of the table.

IP Address / FQDN	Port	Transport
192.218.23.33	5061	TLS

For the compliance test, there were two SIP server profiles: **Recorder1** and **Recorder2** created for the Cogito recording servers. The screenshot shows the **Edit SIP Server Profile - General** tab parameters as follow.

- Set **Server Type** to **Recording Server**.
- Leave blank for **SIP Domain** and **DNS Query**.
- Set **TLS Client Profile** to the TLS profile for client as defined in **Section 7.3.3**.
- Enter a valid combination of **IP Address / FQDN**, **Port** and **Transport** that the Cogito recording server will use to listen for SIP requests. The standard SIP UDP/TCP port is 5060. The standard SIP TLS port is 5061.

Edit SIP Server Profile - General X

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type: Recording Server ▼

SIP Domain:

DNS Query Type: NONE/A ▼

TLS Client Profile: TLS_Client_Profile ▼

Add

IP Address / FQDN	Port	Transport	
192.218.23.33	5061	TLS ▼	Delete

Finish

In the **Heartbeat** tab, enter following parameters as shown in the screenshot below.

- **Enable Heartbeat:** checked.
- **Method:** select **OPTIONS** in the dropdown menu.
- **Frequency:** enter an interval for the Avaya SBCE sending out OPTIONS to the Cogito recording server.
- **From URI:** enter the uri format as user@domain or user@ipaddress. In the testing, the public IP for SIPREC was used in “**From**” header in OPTIONS message sent to Cogito.
- **To URI:** enter the uri format as user@ipaddress with the IP address of the Cogito recording server.

Edit SIP Server Profile - Heartbeat X

Enable Heartbeat ☒

Method: OPTIONS ▼

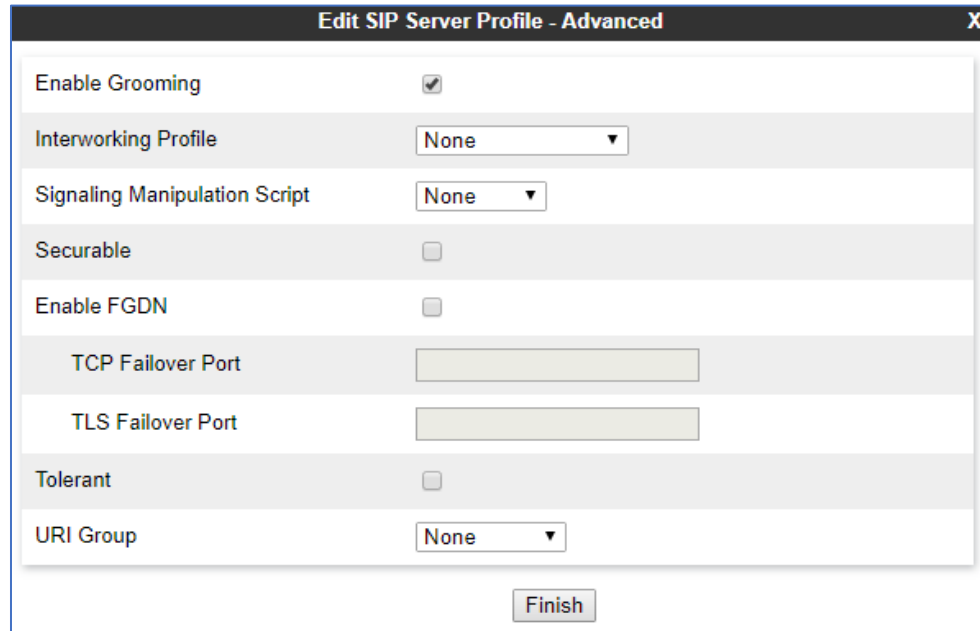
Frequency: 60 seconds

From URI: siprec@10.207.80.109

To URI: siprec@192.218.23.33

Finish

In the **Advanced** tab, check on the **Enable Grooming** checkbox and keep other fields as default.



Edit SIP Server Profile - Advanced

Enable Grooming ☒

Interworking Profile None

Signaling Manipulation Script None

Securable ☐

Enable FGDN ☐

TCP Failover Port

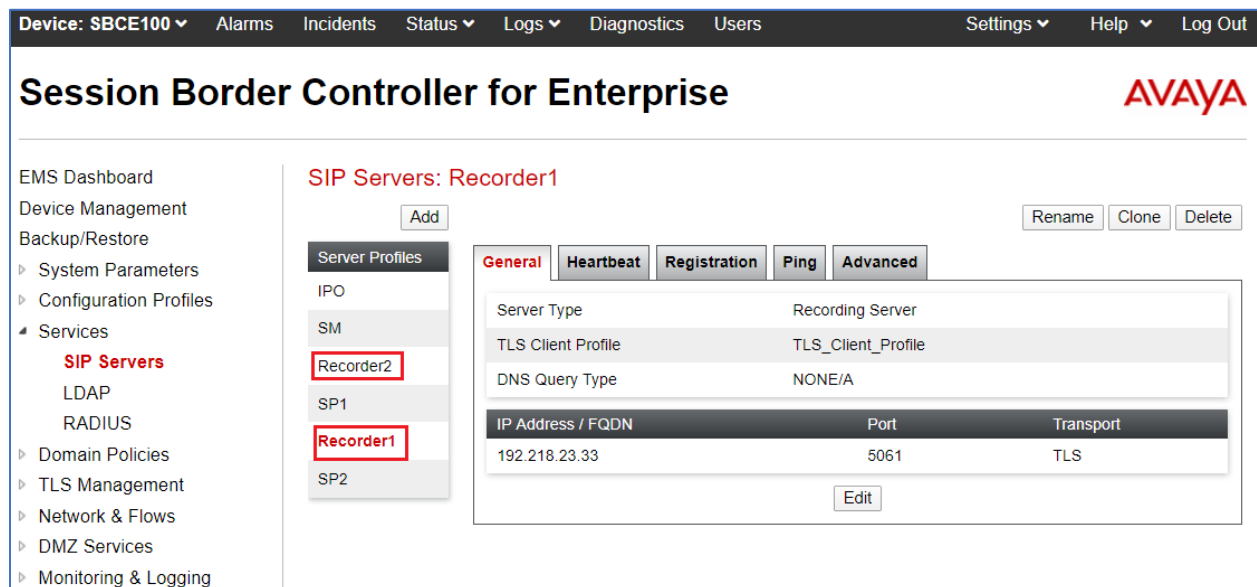
TLS Failover Port

Tolerant ☐

URI Group None

Finish

Repeat the procedure above to create additional SIP servers as required. The screen below shows the 2 SIP servers for the Cogito recording servers.



Device: SBCE100 Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
 SIP Servers
 LDAP
 RADIUS
Domain Policies
TLS Management
Network & Flows
DMZ Services
Monitoring & Logging

SIP Servers: Recorder1

Add **Rename** **Clone** **Delete**

Server Profiles

- IPO
- SM
- Recorder2**
- SP1
- Recorder1**
- SP2

General **Heartbeat** **Registration** **Ping** **Advanced**

Server Type Recording Server

TLS Client Profile TLS_Client_Profile

DNS Query Type NONE/A

IP Address / FQDN	Port	Transport
192.218.23.33	5061	TLS

Edit

7.7. Routing Configuration

A routing profile defines where traffic will be directed based on the contents of the Request-URI. To create a new profile, navigate to **Configuration Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by one or more pop-up windows in which the profile parameters can be configured.

For the compliance test, routing profile **To-Recorder** was created for the Cogito recording server. The screenshot bellows shows the parameters for the routing profile to Cogito.

- Set the **URI Group** to the wild card “*” to match on any URI.
- Set **Load Balancing** to **Round-Robin** from the pull-down menu.
- Click **Add** to enter the following for the Next Hop Address:
 - For **SIP Server Profile**, select two SIP server profiles **Recorder1** and **Recorder2** (Section 7.6) from the pull-down menu. The **Next Hop Address** will be filled-in automatically.
- Keep other parameters as default.

Click **Finish**.

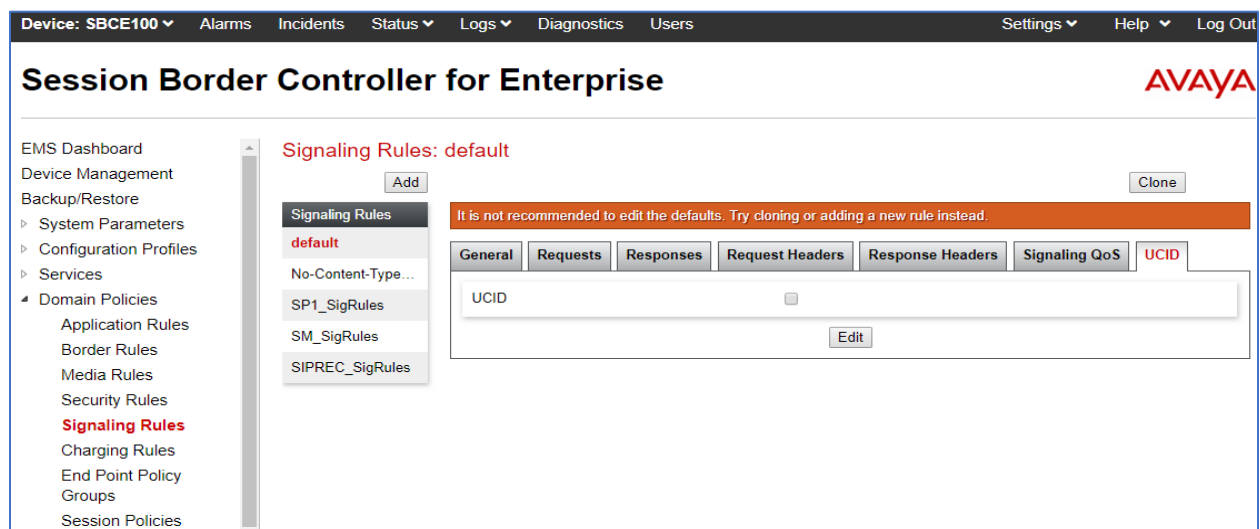
URI Group	Time of Day	Load Balancing	NAPTR	Transport	LDAP Routing	LDAP Server Profile	LDAP Base DN (Search)	Matched Attribute Priority	Alternate Routing	Next Hop Priority	Next Hop In-Dialog	Ignore Route Header	ENUM	ENUM Suffix
*	default	Round-Robin	<input type="checkbox"/>	None	<input type="checkbox"/>	None	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	Delete
1				Recorder1	192.218.23.33:5061	None	Delete
				Recorder2	192.217.121.209:5061	None	Delete

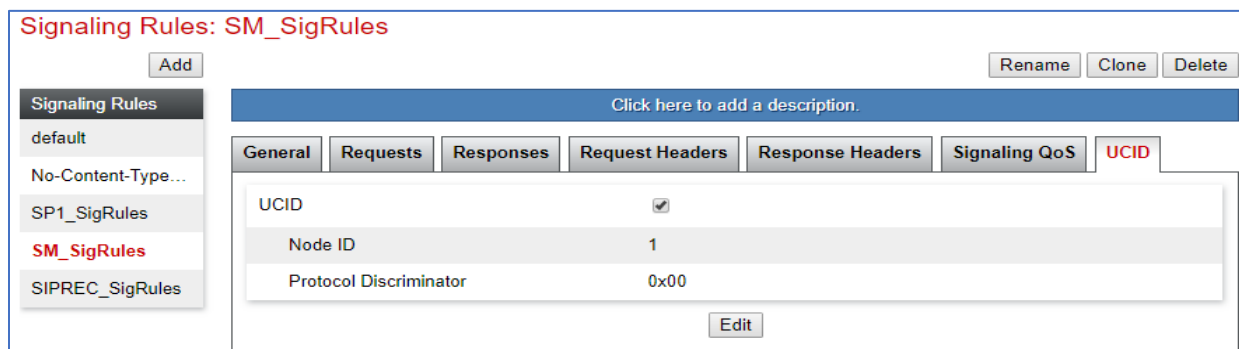
7.8. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.9**. A specific signaling rule was created for Session Manager, Service Provider, and the Cogito recording server.

To create a new rule, navigate to **Domain Policies** → **Signaling Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by one or more pop-up windows in which the rule parameters can be configured. Note that the signaling rules can be also cloned from the default signaling rules by select the **default** in the **Signaling Rules** central column and then click on **Clone** button.



In the testing, there are 3 signaling rules created: **SM_SigRules** and **SP1_SigRules** are previously created for the SIP trunk, and **SIPREC_SigRules** is created for the Cogito recording server. The Signaling rule for Session Manager must have UCID enabled and set the ID number as the same number as the UCID configured in Communication Manager in **Section 5.9**. The screenshot below shows the signaling rules of Session Manager with UCID enabled. Note that UCID in the Service Provider and SIPREC does not need to be enabled; only UCID in the SM signaling rule is required.



7.9. End Point policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and an endpoint (connected server). Thus, an endpoint policy group must be created for Session Manager, Service Provider and the Cogito recording server.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by one or more of pop-up windows in which the group parameters can be configured.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Device: SBCE100', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo on the right. The left sidebar contains a tree view with categories like 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies' (expanded), 'Application Rules', 'Border Rules', 'Media Rules', 'Security Rules', 'Signaling Rules', 'Charging Rules', 'End Point Policy Groups' (highlighted), 'Session Policies', 'TLS Management', and 'Network & Flows'. The main content area shows the 'Policy Groups' section with an 'Add' button and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new group instead.' Below this, a table lists existing policy groups. The table has columns: Order, Application, Border, Media, Security, Signalling, Charging, and RTP Mon Gen. The first row shows a policy group with Order 1, Application 'default', Border 'default', Media 'default-low-med', Security 'default-low', Signalling 'default', Charging 'None', and RTP Mon Gen 'Off'. An 'Edit' link is visible next to the last column. A 'Summary' button is also present.

Order	Application	Border	Media	Security	Signalling	Charging	RTP Mon Gen
1	default	default	default-low-med	default-low	default	None	Off

In the testing, there are 3 end point policy groups created: **SM_EPG** and **SP1_EPG** are previously created for the SIP trunk, and **SIPREC_EPG** is created for the Cogito recording server.

The screenshot below shows the end point policy groups used for Session Manager, **SM_EPG**. The policy group uses the **SM_SigRules** created in **Section 7.8** above.

Policy Groups: SM_EPG

Add Rename Clone Delete

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- avaya-def-low-enc
- avaya-def-high-sub...
- avaya-def-high-server
- SM_EPG**
- SP1_EPG
- SIPREC_EPG

Click here to add a description.

Click here to add a row description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default-trunk	default	SM_MedRules	default-low	SM_SigRules	None	Off	Edit

The screenshot below shows the end point policy groups used for Service Provider, **SP1_EPG**. The policy group uses the **SP1_SigRules** created in **Section 7.8** above.

Policy Groups: SP1_EPG

Add Rename Clone Delete

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- avaya-def-low-enc
- avaya-def-high-sub...
- avaya-def-high-server
- SM_EPG
- SP1_EPG**
- SIPREC_EPG

Click here to add a description.

Click here to add a row description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default-trunk	default	default-low-med	default-low	SP1_SigRules	None	Off	Edit

The screenshot below shows the end point policy groups used for the Cogito recording server, **SIPREC_EPG**. The policy group uses the **SIPREC_SigRules** created in **Section 7.8** above.

Policy Groups: SIPREC_EPG

Add Rename Clone Delete

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- avaya-def-low-enc
- avaya-def-high-sub...
- avaya-def-high-server
- SM_EPG
- SP1_EPG
- SIPREC_EPG**

Click here to add a description.

Click here to add a row description.

Policy Group Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen
1	default-trunk	default	default-low-med	default-low	SIPREC_SigRules	None	Off

Edit

7.10. Session Policies

To create a new session policy group, navigate to **Domain Policies** → **Session Policies** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by one or more of pop-up windows in which the group parameters can be configured.

Device: SBCE100 Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise **AVAYA**

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Charging Rules
End Point Policy Groups
Session Policies

Session Policies: default Add Clone

Session Policies

- default
- SIPREC_SessP...

It is not recommended to edit the defaults. Try cloning or adding a new policy instead.

Media

Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None
Converged Conferencing	<input type="checkbox"/>
Recording Server	<input type="checkbox"/>
Media Server	<input type="checkbox"/>

Edit

In the testing, the session policy **SIPREC_SessPolicy** is created with configuration as shown below.

- **Media Anchoring**: checked.
- **Recording Server**: checked.
- **Recording Type**: select **Full Time** in the dropdown menu.
- **Routing Profile**: select the routing profile **To-Recorder** as configured in **Section 7.7**.

Session Policies: SIPREC_SessPolicy

Add

RenameCloneDelete

Session Policies

default

SIPREC_SessP...

Click here to add a description.

Media

Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None
Converged Conferencing	<input type="checkbox"/>
Recording Server	<input checked="" type="checkbox"/>
Recording Type	Full Time
Play Recording Tone	<input type="checkbox"/>
Call Termination on Recording Failure	<input type="checkbox"/>
Routing Profile	To-Recorder
Media Server	<input type="checkbox"/>

Edit

7.11. Session Flows

To create a new rule, navigate to **Network & Flows** → **Session Flow** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by one or more pop-up windows in which the rule parameters can be configured.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: SBCE100', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left sidebar lists various management options, with 'Network & Flows' expanded to show 'Session Flows' in red. The main content area is titled 'Session Flows' and contains an 'Add' button, a warning message, a description link, and a table of existing session flows.

Priority	Flow Name	URI Group #1	URI Group #2	Subnet #1	Subnet #2	Session Policy	
1	SIPREC Session Flow	*	*	*	*	SIPREC_SessPolicy	Clone Edit Delete

In the testing, the session flow **SIPREC Session Flow** is created with the configuration as shown below.

- **Flow Name:** enter a descriptive name.
- **Session Policy:** select the session policy *SIPREC_SessPolicy* in the dropdown menu as configured in **Section 7.10**.
- Keep other fields at default values.

The screenshot shows a configuration window titled "Edit Flow: SIPREC Session Flow". The window contains the following fields and controls:

- Flow Name:** A text input field containing "SIPREC Session Flow".
- URI Group #1:** A dropdown menu with a single visible option marked with an asterisk (*).
- URI Group #2:** A dropdown menu with a single visible option marked with an asterisk (*).
- Subnet #1:** A text input field containing an asterisk (*). Below it, the text "Ex: 192.168.0.1/24" is displayed.
- SBC IP Address:** A dropdown menu with a single visible option marked with an asterisk (*).
- Subnet #2:** A text input field containing an asterisk (*). Below it, the text "Ex: 192.168.0.1/24" is displayed.
- SBC IP Address:** A dropdown menu with a single visible option marked with an asterisk (*).
- Session Policy:** A dropdown menu with "SIPREC_SessPolicy" selected.
- Has Remote SBC:** A checkbox that is currently unchecked.
- Finish:** A button located at the bottom right of the window.

7.12. End Point Flows

Endpoint flows are used to determine the endpoints (connected servers) involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied.

To create a new flow for a server endpoint, navigate to **Network & Flows** → **End Point Flows** in the left pane. In the right pane, select the **Server Flows** tab and click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters.

Device: SBCE100 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

End Point Flows

Subscriber Flows **Server Flows**

Add

Modifications made to a Server Flow will only take effect on new sessions.

Click here to add a row description.

SIP Server: Recorder

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	SIPREC For SM	*	Public1_Sig	Public_SIPREC_Sig	SIPREC_EPG	To-Recorder View Clone
2	SIPREC for SP	*	Private1_Sig	Public_SIPREC_Sig	SIPREC_EPG	To-Recorder View Clone

SIP Server: SM

In the testing, there were totally four server flows created for two Cogito recording servers to record both ways from the PSTN to the enterprise (agent device) and from the enterprise (agent device) to the PSTN via the SIP trunk.

The screenshot below shows the configuration for the Cogito Recorder1 server flow from Session Manager toward the service provider, **Recorder1 For SM**:

- **Flow Name:** enter a descriptive name, e.g. **Recorder1 For SM**.
- **SIP Server Profile:** select **Recorder1** as configured in **Section 7.6**.
- **Received Interface:** select **Public1_Sig** in the list. This is the interface receiving the signaling for the server flow from Session Manager to the service provider.

- **Signaling Interface:** select *Public_SIPREC_Sig* as configured in **Section 7.4**.
- **Media Interface:** select *Public_SIPREC_Med* as configured in **Section 7.5**.
- **End Point Policy Group:** select **SIPREC_EPG** as configured in **Section 7.9**.
- **Routing Profile:** select *To-Recorder* as configured in **Section 7.7**.
- Keep other fields at the default values.

Edit Flow: Recorder1 For SM
X

Flow Name	Recorder1 For SM
SIP Server Profile	Recorder1 ▼
URI Group	* ▼
Transport	* ▼
Remote Subnet	*
Received Interface	Public1_Sig ▼
Signaling Interface	Public_SIPREC_Sig ▼
Media Interface	Public_SIPREC_Med ▼
Secondary Media Interface	None ▼
End Point Policy Group	SIPREC_EPG ▼
Routing Profile	To-Recorder ▼
Topology Hiding Profile	default ▼
Signaling Manipulation Script	None ▼
Remote Branch Office	Any ▼
Link Monitoring from Peer	<input type="checkbox"/>

Finish

The screenshot below shows the configuration for the Cogito Recorder1 server flow from the Service Provider toward Session Manager, **Recorder1 For SP**:

- **Flow Name**: enter a descriptive name, e.g. **Redorder1 For SP**.
- **SIP Server Profile**: select **Recorder** as configured in **Section 7.6**.
- **Received Interface**: select **Private1_Sig** in the list. This is the interface receiving the signaling for the server flow from the service provider toward to Session Manager.
- **Signaling Interface**: select **Public_SIPREC_Sig** as configured in **Section 7.4**.
- **Media Interface**: select **Public_SIPREC_Med** as configured in **Section 7.5**.
- **End Point Policy Group**: select **SIPREC_EPG** as configured in **Section 7.9**.
- **Routing Profile**: select **To-Recorder** as configured in **Section 7.7**.
- Keep other fields at the default values.

Edit Flow: Recorder1 for SP	
Flow Name	Recorder1 for SP
SIP Server Profile	Recorder1 ▼
URI Group	* ▼
Transport	* ▼
Remote Subnet	*
Received Interface	Private1_Sig ▼
Signaling Interface	Public_SIPREC_Sig ▼
Media Interface	Public_SIPREC_Med ▼
Secondary Media Interface	None ▼
End Point Policy Group	SIPREC_EPG ▼
Routing Profile	To-Recorder ▼
Topology Hiding Profile	default ▼
Signaling Manipulation Script	None ▼
Remote Branch Office	Any ▼
Link Monitoring from Peer	<input type="checkbox"/>
Finish	

The screenshot below shows the configuration for the Cogito Recorder2 server flow from Session Manager toward the Service Provider, **Recorder2 For SM**:

All the values are set as the same as the server flow for the Cogito Recorder1 server, except for the **SIP Server Profile** field, select **Recorder2** in the dropdown menu.

Edit Flow: Recorder2 For SM	
Flow Name	Recorder2 For SM
SIP Server Profile	Recorder2 ▼
URI Group	* ▼
Transport	* ▼
Remote Subnet	*
Received Interface	Public1_Sig ▼
Signaling Interface	Public_SIPREC_Sig ▼
Media Interface	Public_SIPREC_Med ▼
Secondary Media Interface	None ▼
End Point Policy Group	SIPREC_EPG ▼
Routing Profile	To-Recorder ▼
Topology Hiding Profile	default ▼
Signaling Manipulation Script	None ▼
Remote Branch Office	Any ▼
Link Monitoring from Peer	<input type="checkbox"/>
Finish	

The screenshot below shows the configuration for the Cogito Recorder2 server flow from the Service Provider toward Session Manager, **Recorder2 For SP**:

All the values are set as the same as the server flow for the Cogito Recorder1 server, except for the **SIP Server Profile** field, select **Recorder2** in the dropdown menu

Edit Flow: Recorder2 For SP	
Flow Name	Recorder2 For SP
SIP Server Profile	Recorder2 ▼
URI Group	* ▼
Transport	* ▼
Remote Subnet	*
Received Interface	Private1_Sig ▼
Signaling Interface	Public_SIPREC_Sig ▼
Media Interface	Public_SIPREC_Med ▼
Secondary Media Interface	None ▼
End Point Policy Group	SIPREC_EPG ▼
Routing Profile	To-Recorder ▼
Topology Hiding Profile	default ▼
Signaling Manipulation Script	None ▼
Remote Branch Office	Any ▼
Link Monitoring from Peer	<input type="checkbox"/>
Finish	

8. Configure Cogito Recording

The Cogito Dialog solution is installed and deployed in the cloud. The configuration of the Cogito recording server and its related applications are done by Cogito technical engineer therefore it is not documented in the Application Notes. For more information about the Cogito recording solution, please contact Cogito Support directly.

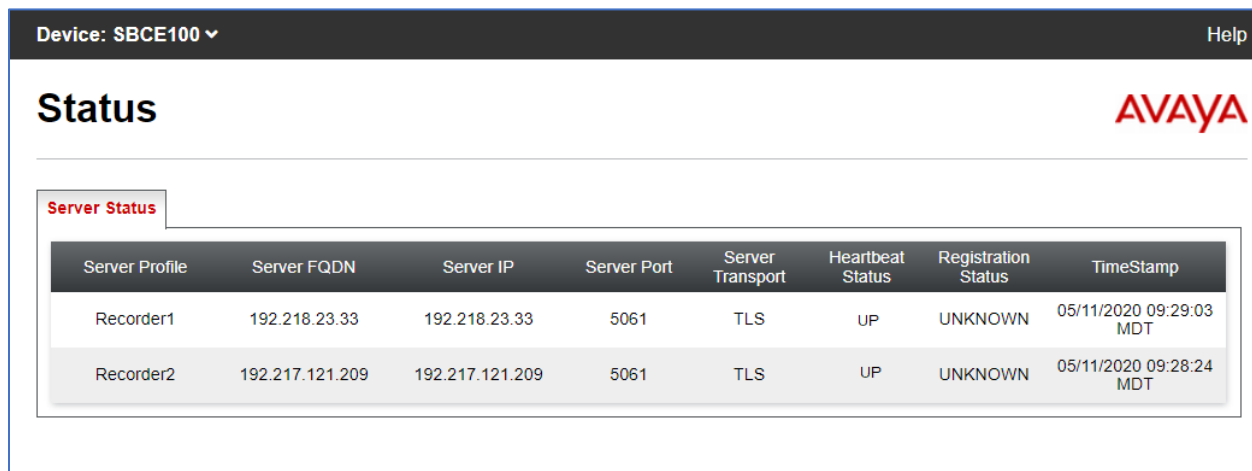
For configuring TLS, the certificate authority (CA) of System Manager is used to create the certificate for the Cogito SIP recording server.

9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

9.1. Verify Server Status in SBCE

Verify the status of the Cogito recording servers in the Avaya SBCE, from the horizontal menu navigate to **Status** → **Server Status** (not shown). The status in the **Heartbeat Status** column should display as “UP”.



The screenshot shows the Avaya SBCE interface. At the top, there is a header bar with "Device: SBCE100" on the left and "Help" on the right. Below the header, the word "Status" is displayed in large font on the left, and the "AVAYA" logo is on the right. A tab labeled "Server Status" is selected. Below the tab is a table with the following data:

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Recorder1	192.218.23.33	192.218.23.33	5061	TLS	UP	UNKNOWN	05/11/2020 09:29:03 MDT
Recorder2	192.217.121.209	192.217.121.209	5061	TLS	UP	UNKNOWN	05/11/2020 09:28:24 MDT

9.2. Verify AES Connection

Verify the status of the **TSAPI Service Summary** service by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** is displayed in the right pane. The status should be in “**Talking**” in the **Status** column.

The screenshot shows the 'TSAPI Link Details' page. The left navigation pane has 'Status' expanded, and 'Status and Control' is selected. Under 'Status and Control', 'TSAPI Service Summary' is highlighted. The main content area shows 'TSAPI Link Details' with a refresh toggle set to 60 seconds. A table displays link information:

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	interopcm	2	Talking	Fri Aug 30 21:19:17 2019	Online	18	4	15	15	30

Below the table are 'Online' and 'Offline' buttons. A section for service-wide information includes buttons for 'TSAPI Service Status', 'TLink Status', and 'User Status' (which is highlighted with a red box).

Select the **User Status** button in the **TSAPI Link Details** page above to show the status of CTI user used for TSAPI service. The **CTI User Status** displays the *cogito* CTI user name with the time of the connection established.

The screenshot shows the 'CTI User Status' page. The left navigation pane is the same as the previous screenshot. The main content area shows 'CTI User Status' with a refresh toggle set to 60 seconds. It displays 'CTI Users' as 'All Users' and 'Submit'. Below this, it shows 'Open Streams: 1' and 'Closed Streams: 50'. A section for 'Open Streams' contains a table:

Name	Time Opened	Time Closed	Tlink Name
cogito	Sat 28 Mar 2020 04:59:01 AM IST		AVAYA#INTEROPCM#CSTA#AES81

Below the table are buttons for 'Show Closed Streams', 'Close All Opened Streams', and 'Back'.

9.3. Verify Status of Agent in CM

Use the command “**list monitored-station**” to verify the Cogito JTAPI client is able to establish a connection with Application Enablement TSAPI service and monitor agent extensions in Communication Manager. The CTI link number should be matched with the CTI link as configured in **Section 5.2**.

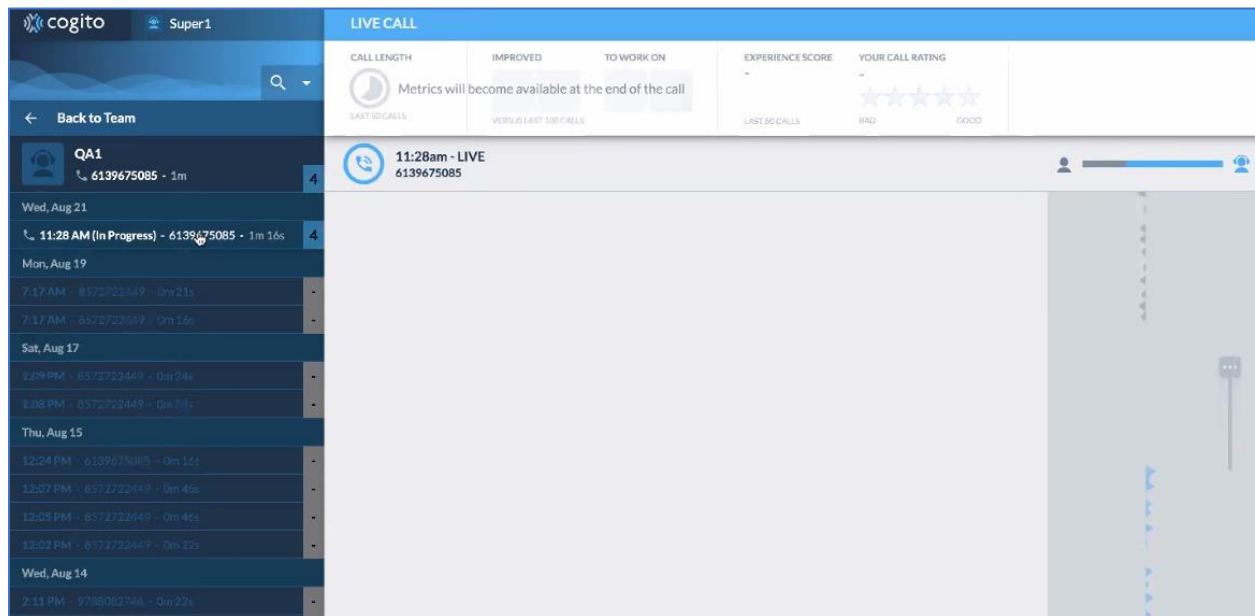
list monitored-station																
MONITORED STATION																
Associations:		1		2		3		4		5		6		7		8
		CTI		CTI		CTI		CTI		CTI		CTI		CTI		CTI
Station Ext		Lnk CRV		Lnk CRV		Lnk CRV		Ltnk CRV		Lnk CRV		Lnk CRV		Lnk CRV		Lnk
CRV																
-----		-----		-----		-----		-----		-----		-----		-----		-----
3301		2 0001														
3303		2 0002														
3401		2 0004														
3403		2 0003														

Use the command “**list agent-loginID**” to verify the status of agent. Note that the agents need to be logged in for Cogito recording server to trigger the recording.

list agent-loginID									
AGENT LOGINID									
Login ID	Name		Extension		Dir	Agt	AAS/AUD		COR AgPr SO
	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv			Skil/Lv	Skil/Lv	
1000	Agent	1000	3301						1 lv1
	1/01	/	/	/					
1001	Agent	1001	3401						1 lv1
	1/01	/	/	/					
1002	Agent	1002	3403						1 lv1

9.4. Verification Steps for SIPREC:

1. Place a call from PSTN to contact center queue via the SIP trunk through the Avaya SBCE and Session Manager and the call arrives to an available agent.
2. Answer the contact center call on the agent.
3. Verify the Cogito recording server receives a live recording call from the Avaya SBCE as shown in the screen below.



4. Disconnect the contact center call from the PSTN user. Verify the Avaya SBCE sends Bye message to the Cogito recording server and receive responses from Cogito to end the recording call.

10. Conclusion

These Application Notes describe the configuration steps required for Cogito Dialog to successfully interoperate with Avaya Aura® Application Enablement Services and Avaya Session Border Controller for Enterprise. All feature and serviceability test cases were completed with observations noted in **Section** Error! Reference source not found..

11. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Deploying Avaya Aura® applications from System Manager*, Release 8.1, October 2019
- [2] *Deploying Avaya Aura® Communication Manager*, Release 8.1, October 2019
- [3] *Administering Avaya Aura® Communication Manager*, Release 8.1, October 2019
- [4] *Deploying Avaya Aura® Session Manager*, Release 8.1 October 2019
- [5] *Upgrading Avaya Aura® Session Manager* Release 8.1, October 2019
- [6] *Administering Avaya Aura® Session Manager* Release 8.1, October 2019
- [7] *Deploying Avaya Session Border Controller for Enterprise Release 8.1*, February 2020
- [8] *Upgrading Avaya Session Border Controller for Enterprise Release 8.1*, February 2020
- [9] *Administering Avaya Session Border Controller for Enterprise Release 8.1*, February 2020

©2020 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.