



DevConnect Program

Application Notes for Cogito Emotion AI with Avaya Aura® Application Enablement Services 10.1 and Avaya Session Border Controller 10.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cogito Emotion AI to interoperate with Avaya Aura® Application Enablement Services and Avaya Session Border Controller using TLS and SRTP. Cogito Emotion AI is a cloud-based 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 Avaya DevConnect Program.

1. Introduction

These Application Notes describe the configuration steps required for Cogito Emotion AI to interoperate with Avaya Aura® Application Enablement Services and Avaya Session Border Controller (Avaya SBC) using TLS and SRTP. Cogito Emotion AI is a cloud-based SIPREC call recording and analysis solution.

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

2. General Test Approach and Test Results

The general test approach was to verify the features and serviceability of the Cogito Emotion AI successfully integrate with Application Enablement Services using JTAPI and utilize SIPREC in the Avaya SBC 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 Services using TSAPI services.
- Response to SIP OPTIONS messages.
- Caller ID Presentation.
- Call recording of inbound calls from SIP trunk to elite call center queue and then answered by an available agent.
- Call recording of inbound calls from SIP trunk directly to agent.
- Call recording of outbound calls from agents over 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.
- Serviceability testing – The behavior of Cogito recording server under different failure conditions.

<p>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 this document.</p>
--

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 Emotion AI 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 agent 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.

2.3. Support

Technical support on Cogito Emotion AI 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 SBC to connect to service provider for calls from PSTN to enterprise and vice versa. The Cogito Emotion AI solution established a connection to Application Enablement Services using TSAPI services with a JTAPI client and receives SIP messages and audio call recording from Avaya SBC.

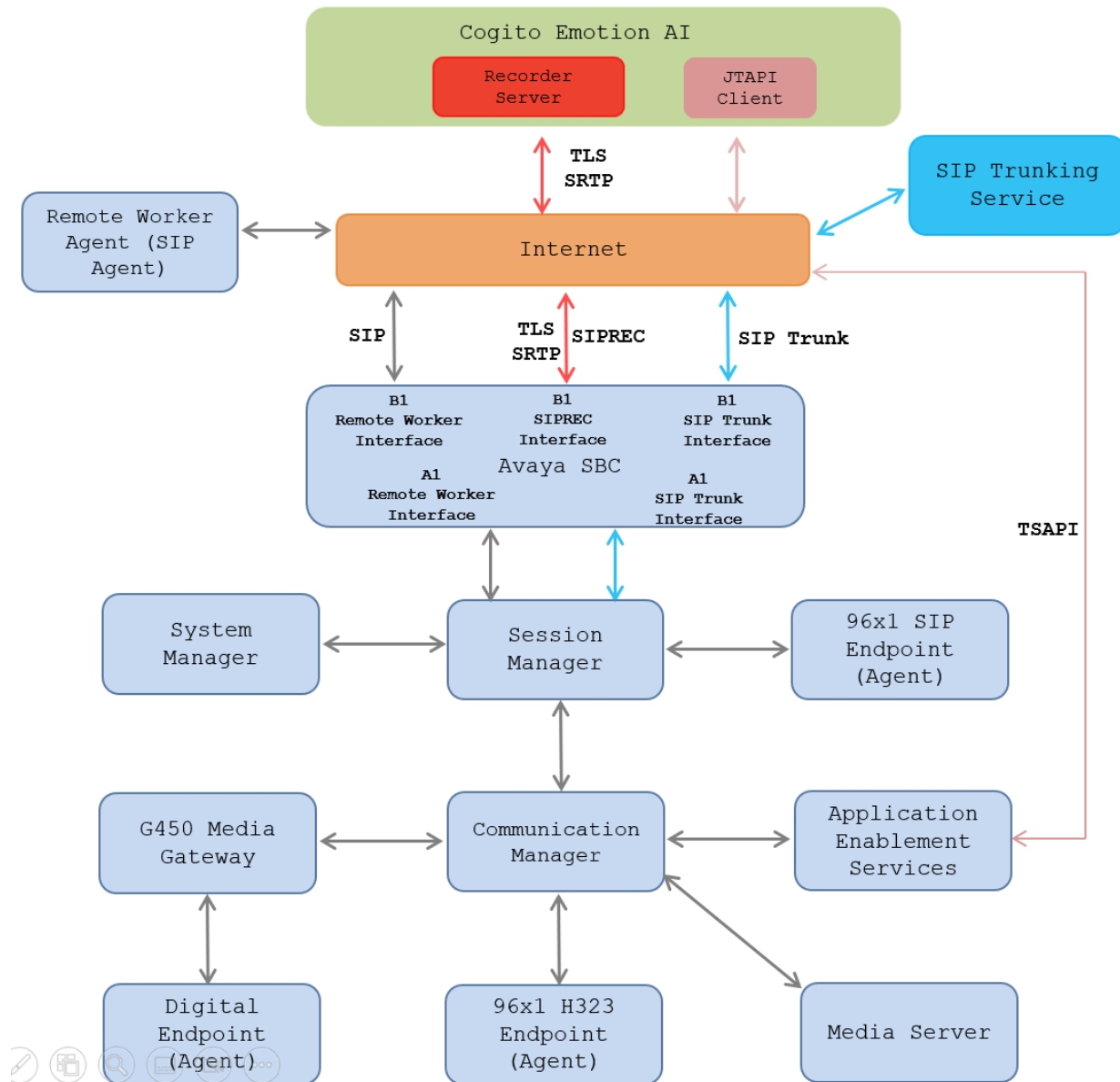


Figure 1: Test Configuration Diagram for Cogito Emotion AI

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

Description	IP Address
System Manager	10.33.1.40
Session Manager	10.33.1.41
Communication Manager	10.33.1.43
Application Enablement Services	10.33.1.14
Session Border Controller	10.33.10.102
Media Server	10.33.1.30
G450 Media Gateway	10.33.1.8
H.323 Endpoints	192.168.11.10-12
SIP Endpoints	192.168.11.8-9
Cogito Recording Server	192.218.23.33
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	10.1.3.0 CM 10.1.3.0.1.974.27893
Avaya Aura® System Manager running on Virtualized Environment	10.1.2.0 Software No: 10.1.2.0.0715476
Avaya Aura® Session Manager running on Virtualized Environment	10.1.2.0 10.1.2.0.1012016
Avaya Aura® Application Enablement Services	10.1.2.0 10.1.2.0.0.12-0
Avaya Session Border Controller	10.1.2.0 10.1.2.0-64-23285
Avaya Aura® Media Server running on Virtualized Environment	10.1.0.154
Avaya G450 Media Gateway	42.7.0
Avaya 96x1 IP Deskphones	6.8.5.4.10 (H.323)
Avaya J189 Deskphone	4.1.0.0.9 (SIP)
Avaya Agent for Desktop (SIP)	2.0.6.25 (SIP)
Avaya 9408 Digital Deskphone	2.0 SP8 (R19)
Cogito Emotion AI <ul style="list-style-type: none">- Core- Compute- Telephony- Web	1.6.0 1.2.6 1.105.1 1.14.1

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager.

5.1. Verify License

Log into 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			
Name:	AES50	COR: 1		
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 set to **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 Type	Enabled	Local Node	Local Port	Remote Node	Remote 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:	aes10	*	y	in use		
2:	aes50	*	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.

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 to route calls to a skill group is shown below. Vector 1 is used for the configuration of the VDN in the next step.

```
change vector 1                                     Page 1 of 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
                                     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 SBC. 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 in red. To its right, the text "Application Enablement Services" is displayed in bold, with "Management Console" underneath it. A thick red horizontal bar spans the width of the page below the header. In the center, there 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 below the login box. At the bottom center of the page, the copyright notice "Copyright © 2009-2019 Avaya Inc. All Rights Reserved." is displayed.

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



Application Enablement Services Management Console

Welcome: User cust
Last login: Tue Aug 8 07:34:55 E.S.T. 2023 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes50/10.33.1.14
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Thu Aug 24 16:19:12 EDT 2023
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.

Copyright © 2009-2023 Avaya Inc. All Rights Reserved.

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.

APS_CMS_Connectors	Licensed Features		
▶APS_CMS_Connectors	14 Items  Show All ▾		
Configure Centralized Licensing			
CE			
▶COLLABORATION_ENVIRONMENT			
CMS			
▶CMS			
Configure Centralized Licensing			
COMMUNICATION_MANAGER			
▶Call_Center			
▶Communication_Manager			
IPO			
▶IP_Office			
OL			
▶OL			
PRESENCE_SERVICES			
▶Presence_Services			
SYSTEM_MANAGER			
▶System_Manager			
SessionManager			

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.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Aug 8 07:34:55 E.S.T. 2023 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes50/10.33.1.14
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Thu Aug 24 16:27:34 EDT 2023
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Home | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Connection Details - cm10

Switch Password

Confirm Switch Password

Msg Period

Provide AE Services certificate to switch

Secure H323 Connection

Processor Ethernet

Enable TLS Certificate Validation

Apply

Cancel

Select the **cm10** switch connection has been added above and selects **Edit PE/CLAN IPs** to add the IP address of the switch connection.

Communication Manager Interface | Switch Connections

Home | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
cm10	Yes	30	1

Edit Connection Edit PE/CLAN IPs Edit Signaling Details Delete Connection Survivability Hierarchy

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.

Communication Manager Interface | Switch Connections

Home | Help | Logout

▸ AE Services

▾ Communication Manager Interface

Switch Connections

▸ Dial Plan

High Availability

▸ Licensing

▸ Maintenance

▸ Networking

▸ Security

▸ Status

▸ User Management

▸ Utilities

▸ Help

Edit Processor Ethernet IP - cm10

10.33.1.43

Add/Edit Name or IP

Name or IP Address	Status
10.33.1.43	In Use

Back

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 console. The left sidebar contains a tree view with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TWS', 'Communication Manager Interface', 'High Availability', and 'Licensing'. Under 'TSAPI', 'TSAPI Links' is selected. The main content 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 “**cm10**” 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 'Edit TSAPI Links' configuration screen. The left sidebar is the same as the previous screenshot. The main content area is titled 'Edit TSAPI Links' and contains the following fields: 'Link' (text input with value '1'), 'Switch Connection' (dropdown menu with value 'cm10'), 'Switch CTI Link Number' (dropdown menu with value '2'), 'ASAI Link Version' (dropdown menu with value '12'), and 'Security' (dropdown menu with value 'Both'). Below these fields are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

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 and 'Security Database' selected, showing 'Control' as the active sub-item. 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 and 'List All Users' selected. 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

AAA; Reviewed:
SPOC 10/11/2023

Avaya DevConnect Application Notes
©2023 Avaya LLC. All Rights Reserved.

23 of 59
Cogito-ASBC-TLS

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

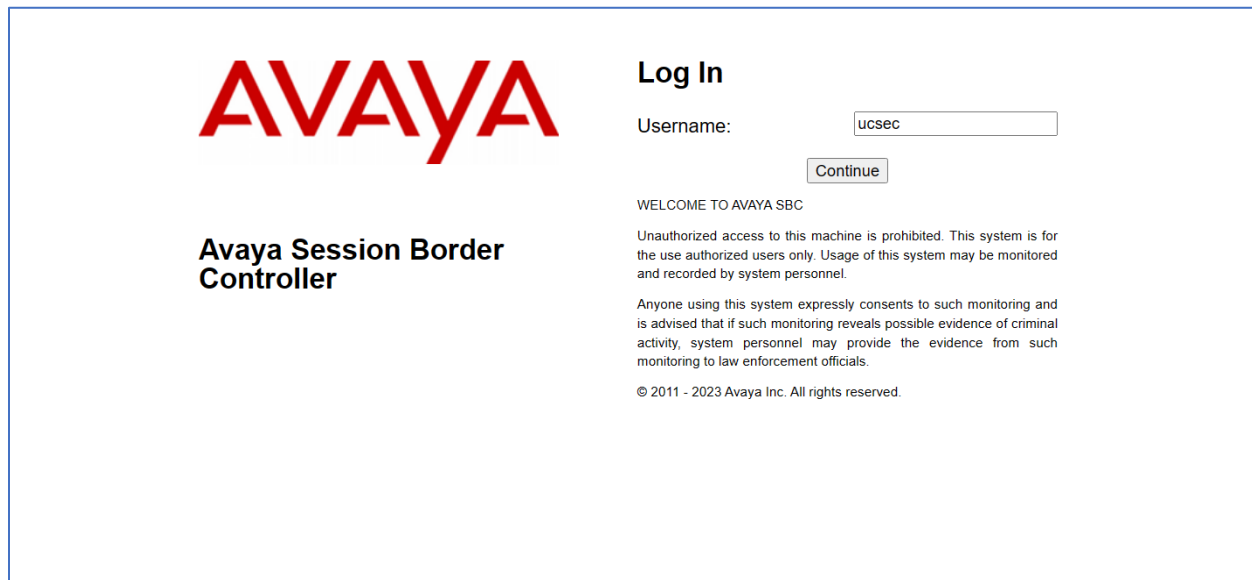
7. Configure Avaya Session Border Controller

This section describes the configuration of the Avaya SBC. It is assumed that the initial installation of the Avaya SBC 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 SBC 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 SBC login page will appear as shown below. Log in with appropriate credentials.



The image shows the Avaya Session Border Controller login page. On the left, there is a large red 'AVAYA' logo and the text 'Avaya Session Border Controller' below it. On the right, there is a 'Log In' section. It includes a 'Username:' label, a text input field containing 'ucsec', and a 'Continue' button. Below the login fields, there is a 'WELCOME TO AVAYA SBC' message, followed by a disclaimer: 'Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.' and a consent statement: 'Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.' At the bottom, it says '© 2011 - 2023 Avaya Inc. All rights reserved.'

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

The screenshot displays the Avaya Session Border Controller Dashboard. The top navigation bar includes 'Device: EMS', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Avaya Session Border Controller' with the AVAYA logo on the right. The left sidebar lists the 'EMS Dashboard' with sub-items: 'Software Management', 'Device Management', 'System Administration', 'Templates', 'Backup/Restore', and 'Monitoring & Logging'. The main content area is titled 'Dashboard' and contains several panels:

- Information:** A table showing system details.

System Time	11:32:13 PM EDT	Refresh
Version	10.1.2.0-64-23285	
GUI Version	10.1.2.0-23278	
Build Date	Tue May 16 08:55:42 IST 2023	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	08/24/2023 23:17:09 EDT	
Failed Login Attempts	0	
- Installed Devices:** A list showing 'EMS' and 'sbc102'.
- Active Alarms (past 24 hours):** A section stating 'None found.'.
- Incidents (past 24 hours):** A list showing two incidents for 'sbc102': 'Heartbeat Successful, Server is UP' and 'Heartbeat Failed, Server is Down'.

An 'Add' button is located at the bottom right of the incidents list.

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**.

The screenshot displays the 'Device Management' screen. The top navigation bar is identical to the dashboard. The left sidebar is also identical. The main content area is titled 'Device Management' and features a sub-navigation bar with 'Devices', 'Updates', 'Licensing', and 'Key Bundles'. The 'Devices' tab is active, showing a table of installed devices:

Device Name	Management IP	Version	Status	
sbc102	10.33.10.102	10.1.2.0-64-23285	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 (**sbc102**). This name will be referenced in other configuration screens. Interface **A1** and **B1** represent the private and public interfaces of the Avaya SBC respectively. Each of these interfaces must be enabled after installation.

System Information: sbc102

General Configuration

Appliance Name	sbc102
Box Type	SIP
Deployment Mode	Proxy
HA Mode	No

Management IP(s)

IP #1 (IPv4)	10.33.10.102
--------------	--------------

DNS Configuration

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

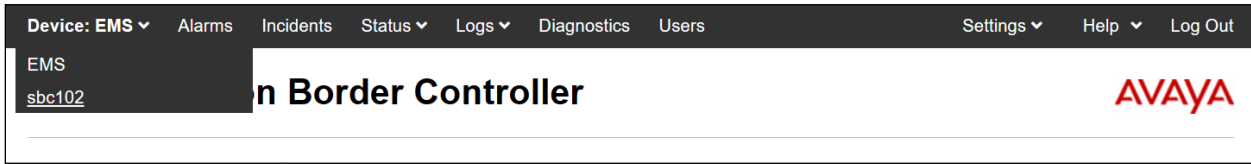
License Allocation

Standard Sessions Requested: 0	0
Advanced Sessions Requested: 0	0
Scopia Video Sessions Requested: 0	0
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 0	0
AMR	<input type="checkbox"/>
Premium Sessions Requested: 0	0
CLID	---
Encryption Available: Yes	<input checked="" type="checkbox"/>

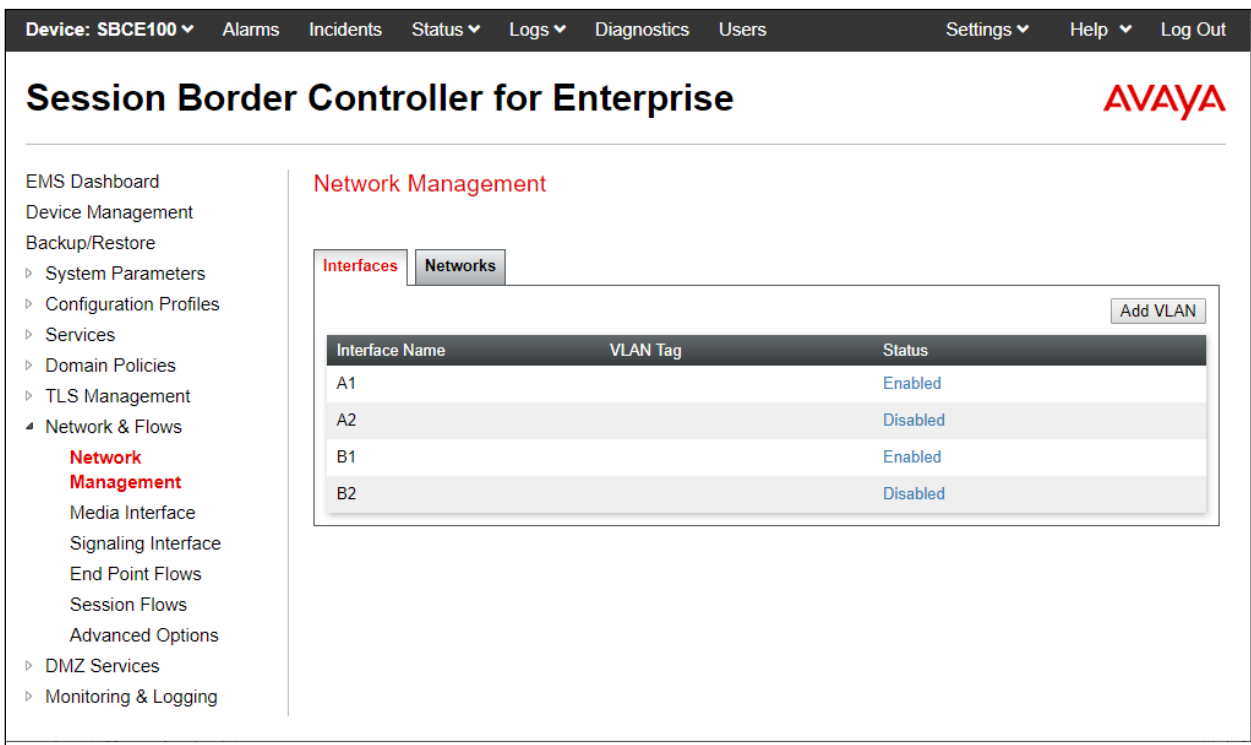
Network Configuration

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
10.33.1.54	10.33.1.54	255.255.255.0	10.33.1.1	A1
10.207.80.90	10.207.80.90	255.255.255.128	10.207.80.1	B1
10.207.80.107	10.207.80.107	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

From the right top corner of the window, select **Device** dropdown menu and select the SBC system, e.g., **sbc102**, 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.



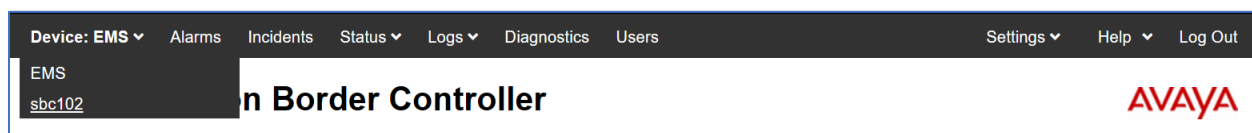
7.3. TLS Management

Note – Testing was done with System Manager signed identity certificates for Cogito recording server and Avaya SBC. 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 SBC and between Avaya SBC and Cogito recording server. The following procedures show how to create the client and server profiles.

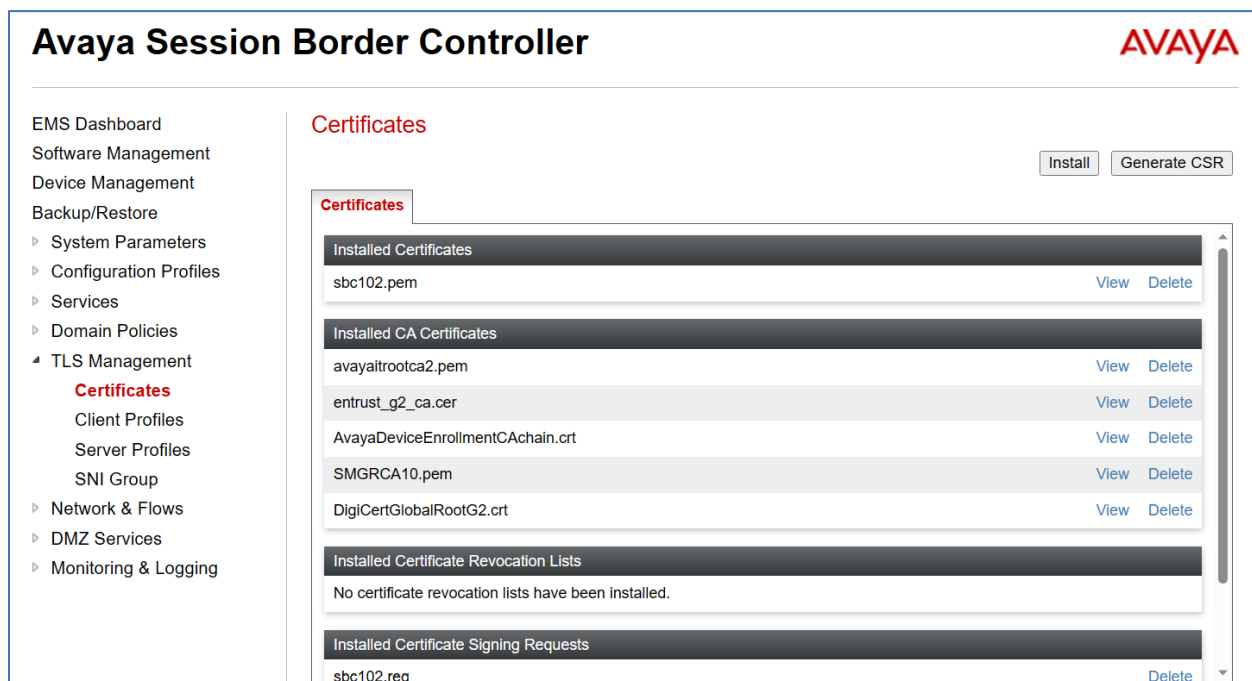
7.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

To access the SBC configuration menus, select the SBC 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., **AvayaSBCServer**).
- **Certificate:** select the identity certificate, e.g., **sbc102.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

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

Edit ProfileX

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

AvayaSBCServer

Certificate

sbc102.pem

SNI Options

None

SNI Group

None

Certificate Verification

Peer Verification

None

Peer Certificate Authorities

avayaitrootca2.pem
entrust_g2_ca.cer
AvayaDeviceEnrollmentCAchain.crt
SMGRCA10.pem

Peer Certificate Revocation Lists

Verification Depth

0

Next

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

The screenshot displays the Avaya Session Border Controller web interface. The top navigation bar includes 'Device: sbc102', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. The left sidebar lists navigation options: EMS Dashboard, Software Management, 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: AvayaSBCServer' and features an 'Add' button and a 'Delete' button. Below the title, there is a blue bar with the text 'Click here to add a description.' The 'Server Profile' section is expanded, showing the following configuration:

TLS Profile	
Profile Name	AvayaSBCServer
Certificate	sbc102.pem
SNI Options	None

Certificate Verification	
Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

7.3.3. Client Profiles

Step 1 - Select **TLS Management** → **Server Profiles** and click on **Add** (not shown). Enter the following:

- **Profile Name:** enter a descriptive name (e.g., **AvayaSBCCClient**)
- **Certificate:** select the identity certificate, e.g., **sbc102.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., **SMGRCA10.pem**.
- Enter 1 under **Verification Depth**. Click **Next**.

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

Edit Profile X

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: AvayaSBCCClient

Certificate: sbc102.pem

SNI: ☐ Enabled

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities: avayaitrootca2.pem, entrust_g2_ca.cer, AvayaDeviceEnrollmentCAchain.crt, SMGRCA10.pem

Peer Certificate Revocation Lists:

Verification Depth: 2

Extended Hostname Verification: ☐

Server Hostname:

Next

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

The screenshot displays the Avaya Session Border Controller (ASBC) web interface. The top navigation bar includes 'Device: sbc102', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo.

On the left, a sidebar menu lists various management options, with 'TLS Management' expanded to show 'Client Profiles'.

The main content area is titled 'Client Profiles: AvayaSBCCClient'. It features an 'Add' button and a 'Delete' button. Below this, a table lists the configuration details for the 'AvayaSBCCClient' profile:

Client Profile	
Click here to add a description.	
TLS Profile	
Profile Name	AvayaSBCCClient
Certificate	sbc102.pem
SNI	<input type="checkbox"/> Enabled
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SMGRCA10.pem
Peer Certificate Revocation Lists	---
Verification Depth	2
Extended Hostname Verification	<input type="checkbox"/>
Renegotiation Parameters	
Renegotiation Time	0

7.4. Signaling Interface

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

To create a new interface, navigate to **Network & Flows → Signaling Interface** in the left pane. In the center pane, select the Avaya SBC device (**sbc102**) 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 SBC will listen on for each transport protocol. For the internal interface, the Avaya SBC was configured to listen for TLS on port 5061. For the external interface, the Avaya SBC 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 "Finish" button at the bottom. The fields are as follows:

Field	Value
Name	Public1_Sig_SIPRec
IP Address	Public1 (B1, VLAN 0) (dropdown) 10.207.80.109 (dropdown)
TCP Port	(empty field) <small>Leave blank to disable</small>
UDP Port	(empty field) <small>Leave blank to disable</small>
TLS Port	5061 <small>Leave blank to disable</small>
TLS Profile	AvayaSBCServer (dropdown)
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	(empty field)

Finish

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
Private1_Sig_RW	10.33.1.52	The private signaling interface for SIP remote worker connects to Session Manager
Public1_Sig_RW	10.50.207.108	The public signaling interface for SIP remote worker connects to SIP remote worker endpoint
Public1_Sig_SIPREC	10.50.207.109	The public signaling interface connects to Cogito recording server

The screenshot below shows the list of signaling interfaces with TLS Server Profiles assigned that were used during the compliance test.

The screenshot shows the Avaya Session Border Controller (SBC) web interface. The top header displays the device name 'sbc102' and various navigation links like Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main title is 'Avaya Session Border Controller' with the AVAYA logo. The left-hand navigation menu includes options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows (selected), Network Management, Media Interface, Signaling Interface (highlighted), End Point Flows, Session Flows, Advanced Options, DMZ Services, and Monitoring & Logging. The main content area is titled 'Signaling Interface' and contains a table of signaling interfaces. The table has columns for Name, Signaling IP Network, TCP Port, UDP Port, TLS Port, and TLS Profile. There are seven rows of data, each representing a different signaling interface. Each row includes 'Edit' and 'Delete' links for configuration management. An 'Add' button is located at the top right of the table.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile
Private1_Sig_SIPRec	10.33.1.53 Private1 (A1, VLAN 0)	5060	---	5061	AvayaSBCServer
Public1_Sig_SIPRec	10.207.80.109 Public1 (B1, VLAN 0)	5060	5060	5061	AvayaSBCServer
Private1_Sig	10.33.1.51 Private1 (A1, VLAN 0)	5060	---	5061	AvayaSBCServer
Private1_Sig_RW	10.33.1.52 Private1 (A1, VLAN 0)	5060	---	5061	AvayaSBCServer
Public1_Sig	10.207.80.107 Public1 (B1, VLAN 0)	5060	---	5061	AvayaSBCServer
Public2_Sig_RW	10.33.100.70 Public2 (B2, VLAN 0)	5060	5060	5061	AvayaSBCServer
Public1_Sig2	10.207.80.90 Public1 (B1, VLAN 0)	5060	---	5061	AvayaSBCServer

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 SBC.

To create a new interface, navigate to **Network &Flows → Media Interface** in the left pane. In the center pane, select the Avaya SBC device (**sbc102**) 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 SBC and the far-end. For the testing, the default port range was used for the SIPREC public media interface.

Edit Media Interface		X
Name	<input type="text" value="Public1_Med_SIPRec"/>	
IP Address	<input type="text" value="Public1 (B1, VLAN 0)"/>	
	<input type="text" value="10.207.80.109"/>	
Port Range	<input type="text" value="35000"/>	<input type="text" value="40000"/>
<input type="button" value="Finish"/>		

For the testing, list of media interfaces was 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
Public1_Med_RW	10.207.80.108	The public media interface for SIP remote worker connects to SIP remote worker endpoint
Public1_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

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

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 displays the Avaya Session Border Controller (ASBC) configuration interface. The top navigation bar includes 'Device: sbc102', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. The left sidebar lists various management options, with 'Services' expanded to show 'SIP Servers'. The main content area is titled 'SIP Servers: Recorder' and features an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. Below these are tabs for 'General', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'General' tab is active, showing a form with the following fields: 'Server Type' (Recording Server), 'TLS Client Profile' (AvayaSBCCClient), and 'DNS Query Type' (NONE/A). Below these is a table with columns 'IP Address / FQDN', 'Port', 'Transport', and 'Whitelist'. The table contains one entry: IP Address / FQDN: 18.211.218.86, Port: 5061, Transport: TLS, and a checked 'Whitelist' checkbox. An 'Edit' button is located at the bottom right of the table.

IP Address / FQDN	Port	Transport	Whitelist
18.211.218.86	5061	TLS	<input checked="" type="checkbox"/>

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 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
AvayaSBCClient ▼

Add

IP Address / FQDN	Port	Transport	Whitelist	
<input style="width: 150px;" type="text" value="18.211.218.86"/>	<input style="width: 50px;" type="text" value="5061"/>	TLS ▼	<input type="checkbox"/>	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 SBC 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

seconds

From URI

To URI

Finish

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

The screenshot shows a dialog box titled "Edit SIP Server Profile - Advanced". It contains several configuration options:

- Enable Grooming**: A checkbox that is checked.
- Interworking Profile**: A dropdown menu set to "None".
- Signaling Manipulation Script**: A dropdown menu set to "None".
- Securable**: An unchecked checkbox.
- Enable FGDN**: An unchecked checkbox.
- TCP Failover Port**: An empty text input field.
- TLS Failover Port**: An empty text input field.
- Tolerant**: An unchecked checkbox.
- URI Group**: A dropdown menu set to "None".

A "Finish" button is located at the bottom right of the dialog box.

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 **Priority** from the pull-down menu.
- Click **Add** to enter the following for the Next Hop Address:
 - For **SIP Server Profile**, select the SIP server profiles **Recorder** (**Section 7.6**) from the pull-down menu. The **Next Hop Address** will be filled-in automatically.
- Set **Priority/Weight** to “1”.
- Set **SIP Server Profile** to the Cogito SIP server.

Keep other parameters as default and click **Finish**.

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

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				Recorder	18.211.218.86:50	None

Delete

Finish

7.8. Media Rules

A media rule defines the processing to be applied to the selected media. For the compliance test, media rules were created for Session Manager, Service Provider and Cogito recording server to use SRTP.

To define the Media Rule for Session Manager, Service Provider, and the recording server, navigate to **Domain Policies** → **Media Rules** in the main menu on the left-hand side. Click on **Add** and enter details in the Media Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name such as **SM10_MedRules**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Set **Preferred Format #2** to **RTP**.
- Uncheck **Encrypted RTCP**.

Default values were used for all other fields. Click **Finish** (not shown).

The screenshot below shows the media rule for the Session Manager.

The screenshot displays the Avaya Session Border Controller web interface. The top navigation bar includes links for Device, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. The left sidebar contains a menu with categories like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules (highlighted), Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups, Session Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Media Rules: SM10_MedRules' and features an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. Below the title is a list of media rules, with 'SM10_MedRules' selected. The configuration details for 'SM10_MedRules' are shown in a table with tabs for Encryption, Codec Prioritization, Advanced, and QoS. The 'Encryption' tab is active, showing settings for Audio Encryption and Video Encryption. The 'Audio Encryption' section includes 'Preferred Formats' (SRTP_AES_CM_128_HMAC_SHA1_80, RTP), 'Encrypted RTCP' (unchecked), 'MKI' (unchecked), 'Lifetime' (Any), 'Interworking' (checked), 'Symmetric Context Reset' (checked), and 'Key Change in New Offer' (unchecked). The 'Video Encryption' section includes 'Preferred Formats' (RTP) and 'Interworking' (unchecked).

Media Rules	Actions
default-low-med	
default-low-med-...	
default-high	
default-high-enc	
avaya-low-med-enc	
SM10_MedRules	
MedRules-RW	
SIPRec_MedRules	
SP2_MedRules	

Encryption	Codec Prioritization	Advanced	QoS
Audio Encryption			
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP		
Encrypted RTCP	<input type="checkbox"/>		
MKI	<input type="checkbox"/>		
Lifetime	Any		
Interworking	<input checked="" type="checkbox"/>		
Symmetric Context Reset	<input checked="" type="checkbox"/>		
Key Change in New Offer	<input type="checkbox"/>		
Video Encryption			
Preferred Formats	RTP		
Interworking	<input type="checkbox"/>		

The screenshot below shows the media rule for the Service Provider.

Device: sbc102 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesDomain PoliciesApplication RulesBorder RulesMedia RulesSecurity RulesSignaling RulesCharging RulesEnd Point PolicyGroupsSession PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & Logging

Media Rules: SP2_MedRules

AddRenameCloneDelete

Media Rules

default-low-meddefault-low-med-...default-highdefault-high-encavaya-low-med-encSM10_MedRulesMedRules-RWSIPRec_MedRulesSP2_MedRules

Click here to add a description.

EncryptionCodec PrioritizationAdvancedQoS

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80RTP
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Formats	RTP
Interworking	<input type="checkbox"/>

The screenshot below shows the media rule for the Cogito recording server.

Device: sbc102 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesDomain PoliciesApplication RulesBorder RulesMedia RulesSecurity RulesSignaling RulesCharging RulesEnd Point PolicyGroupsSession PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & Logging

Media Rules: SIPRec_MedRules

AddRenameCloneDelete

Media Rules

default-low-meddefault-low-med-...default-highdefault-high-encavaya-low-med-encSM10_MedRulesMedRules-RWSIPRec_MedRulesSP2_MedRules

Click here to add a description.

EncryptionCodec PrioritizationAdvancedQoS

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Formats	RTP
Interworking	<input type="checkbox"/>

AAA; Reviewed:
SPOC 10/11/2023

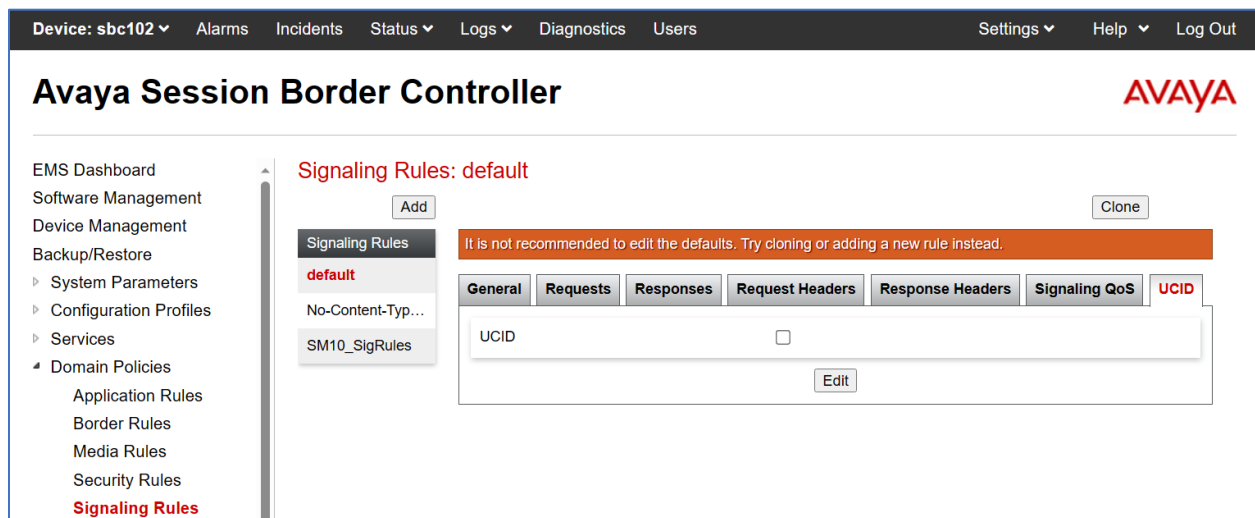
Avaya DevConnect Application Notes
©2023 Avaya LLC. All Rights Reserved.

43 of 59
Cogito-ASBC-TLS

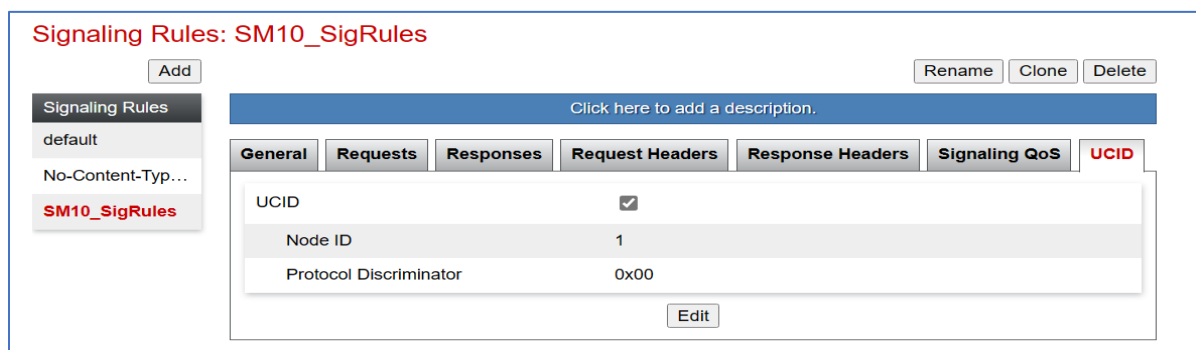
7.9. Signaling Rules

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 7.10**. 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 is one signaling rule created for **SM10_SigRules**, the default signaling rule is used for SIP trunks to service provider and the Cogito recording server. The signaling rules 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 don't need to be enabled; UCID only needs to be enabled for Session Manager Signaling.



7.10. End Point Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBC 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 web interface. The top navigation bar includes 'Device: sbc102', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Avaya Session Border Controller' and the 'AVAYA' logo. The left sidebar contains a tree view with 'Domain Policies' expanded, showing 'End Point Policy Groups' selected. The main content area has an 'Add' button and a 'Clone' button. A message states: 'It is not recommended to edit the defaults. Try cloning or adding a new group instead.' Below this is a table with columns: Order, Application, Border, Media, Security, Signaling, Charging, and RTCP Mon Gen. The table contains one row with the following values: Order 1, Application default, Border default, Media default-low-med, Security default-low, Signaling default, Charging None, and RTCP Mon Gen Off. An 'Edit' link is present next to the last cell. A 'Summary' button is also visible.

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

In the testing, there are three end point policy groups created: **SM_EPG** and **SP2_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, **SM10_EPG**. The policy group uses the **SM10_MedRules** and **SM10_SigRules** created in **Section 7.8** and **7.9** above.

Device: sbc102 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesDomain PoliciesApplication RulesBorder RulesMedia RulesSecurity RulesSignaling RulesCharging RulesEnd Point Policy Groups

Policy Groups: SM10_EPGAddRenameCloneDelete

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen
0	default-trunk	default	SM10_MedRules	default-low	SM10_SigRules	None	Off

The screenshot below shows the end point policy groups used for Service Provider, **SP2_EPG**. The policy group uses the **SP2_MedRules** created in **Section 7.8** above.

Device: sbc102 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesDomain PoliciesApplication RulesBorder RulesMedia RulesSecurity RulesSignaling RulesCharging RulesEnd Point Policy GroupsSession PoliciesTLS ManagementNetwork & FlowsDMZ Services

Policy Groups: SP2_EPGAddRenameCloneDelete

Click here to add a description.

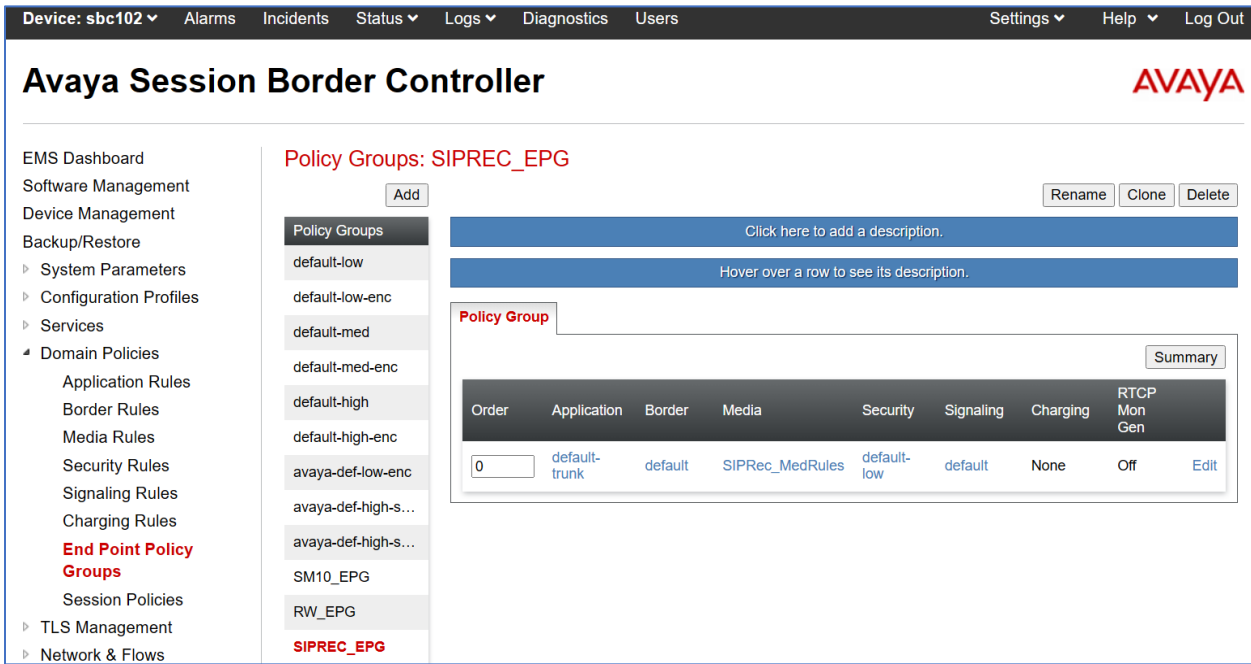
Hover over a row to see its description.

Policy Group

Summary

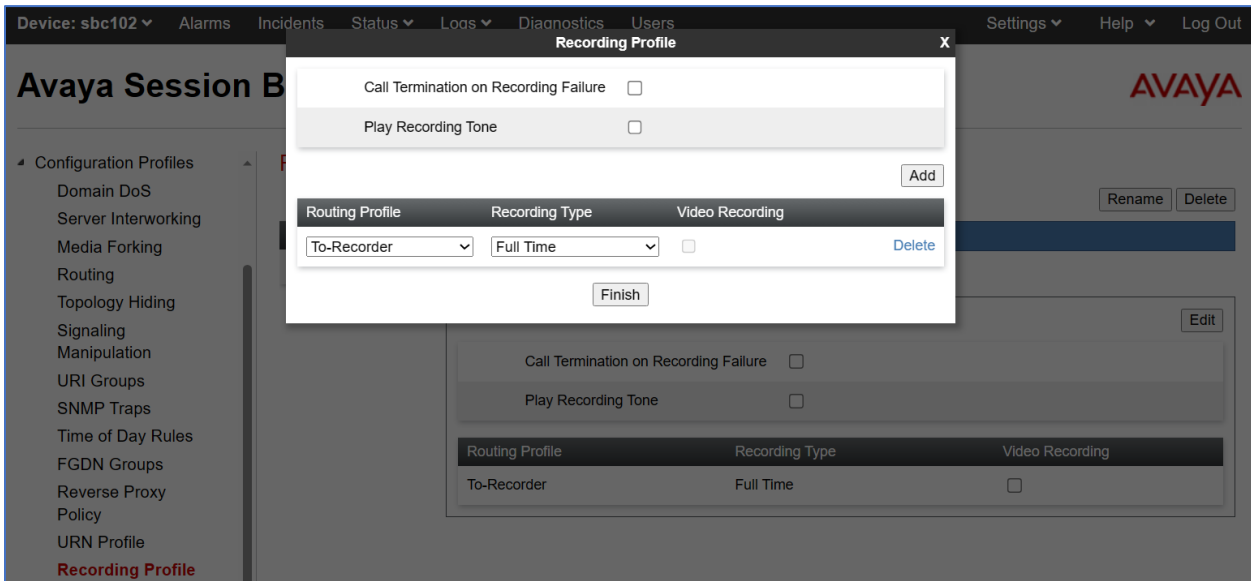
Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen
0	default	default	SP2_MedRules	default-low	default	None	Off

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



7.11. Recording Profiles

To create a recording profile, from the left pane, navigate to **Configuration Profiles** → **Recording Profile**. Select **Add** button (not shown) to add a new recording profile. In the Recording Profile window, select the routing profile as created in **Section 7.7** and select “Full Time” in the **Recording Type**. Select **Finish** to complete.



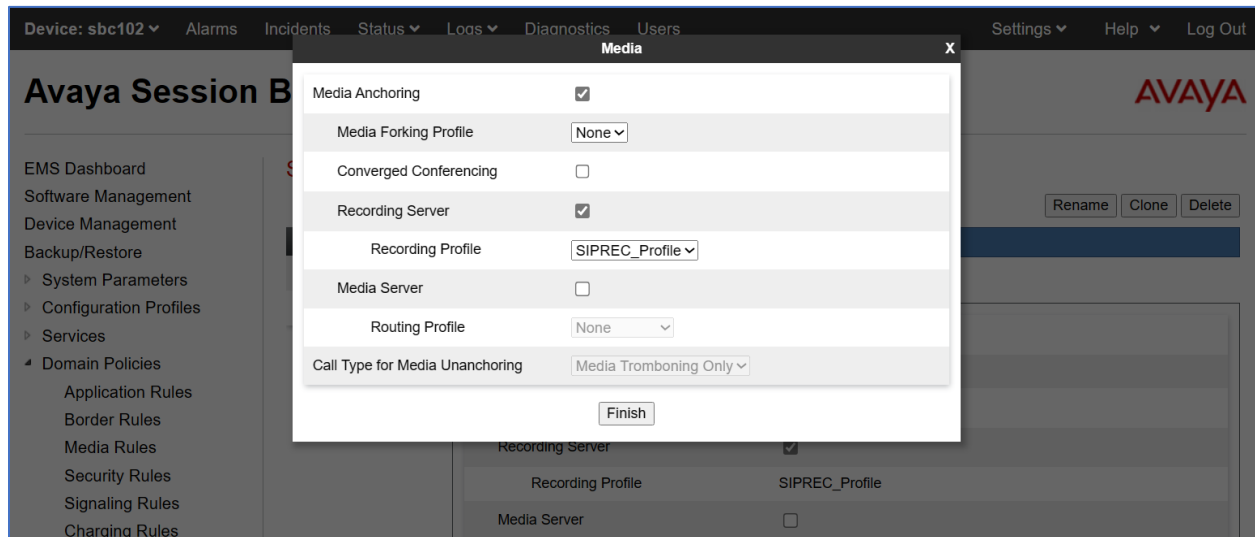
7.12. Session Policies

To create a new session policy group, navigate to **Domain Policies** → **Session Policies** in the left pane. In the center pane, select **Add** (not shown). A pop-up window 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.

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

- **Media Anchoring:** checked.
- **Recording Server:** checked and in the **Recording Profile:** select **SIPREC_Profiles** as created in **Section 7.11** in the dropdown menu.

Keep other fields at default and click **Finish** to complete.



7.13. Session Flows

To create a new flow, navigate to **Network & Flows** → **Session Flow** in the left pane. In the center pane, select **Add** (not shown). A pop-up window displays, enter a descriptive name **SIPREC_SessFlow** in the **Flow Name** field and select the **SIPREC_SessPolicies** as created in **Section 7.12**. Click **Finish** to complete.

The screenshot displays the Avaya Session Border Controller (SBC) configuration interface. The left sidebar shows the navigation menu with 'Session Flows' highlighted under 'Network & Flows'. The main area shows a dialog box titled 'Edit Flow: Recorder_SessFlow' with the following fields:

- Flow Name: SIPREC_SessFlow
- URI Group #1: *
- URI Group #2: *
- Subnet #1: * (Ex: 192.168.0.1/24)
- SBC IP Address: *
- Subnet #2: * (Ex: 192.168.0.1/24)
- SBC IP Address: *
- Session Policy: SIPREC_SessPolicies
- Has Remote SBC: ☐

The 'Finish' button is at the bottom of the dialog box. The background shows the Avaya logo and a list of session policies with 'SIPREC_SessPolicies' selected.

7.14. 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 SBC, 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: sbc102 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

EMS Dashboard
Software Management
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.

Hover over a row to see its description.

SIP Server: Recorder Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Recorder for SM	*	Public1_Sig2	Public1_Sig_SIPRec	SIPREC_EPG	To-Recorder	View Clone Edit Delete
2	Recorder for SP2	*	Private1_Sig2	Public1_Sig_SIPRec	SIPREC_EPG	To-Recorder	View Clone Edit Delete

SIP Server: SM10 Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
----------	-----------	-----------	--------------------	---------------------	------------------------	-----------------

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

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

- **Flow Name:** enter a descriptive name, e.g., **Recorder for SM**.
- **SIP Server Profile:** select **Recorder** as configured in **Section 7.6**.
- **Received Interface:** select **Public1_Sig2** in the list. This is the interface receiving the signaling for the server flow from Session Manager to the service provider.
- **Signaling Interface:** select **Public1_SIPREC_Sig** as configured in **Section 7.4**.

- **Media Interface:** select *Public1_Med_SIPRec* as configured in **Section 7.5**.
- **End Point Policy Group:** select *SIPREC_EPG* as configured in **Section 7.10**.
- **Routing Profile:** select *To-Recorder* as configured in **Section 7.7**.
- Keep other fields at the default values.

Edit Flow: Recorder for SM
X

Flow Name	Recorder for SM
SIP Server Profile	Recorder
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public1_Sig2
Signaling Interface	Public1_Sig_SIPRec
Media Interface	Public1_Med_SIPRec
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"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

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

- **Flow Name:** enter a descriptive name, e.g., **Redorder For SP**.
- **SIP Server Profile:** select ***Recorder*** as configured in **Section 7.6**.
- **Received Interface:** select ***Privarte1_Sig2*** 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 ***Public1_Sig_SIPRec*** as configured in **Section 7.4**.
- **Media Interface:** select ***Public1_Med_SIPRec*** as configured in **Section 7.5**.
- **End Point Policy Group:** select **SIPREC_EPG** as configured in **Section 7.10**.
- **Routing Profile:** select ***To-Recorder*** as configured in **Section 7.7**.
- Keep other fields at the default values.

Edit Flow: Recorder for SP2X

Flow Name	Recorder for SP2
SIP Server Profile	Recorder
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private1_Sig2
Signaling Interface	Public1_Sig_SIPRec
Media Interface	Public1_Med_SIPRec
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"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

8. Configure Cogito Emotion AI

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

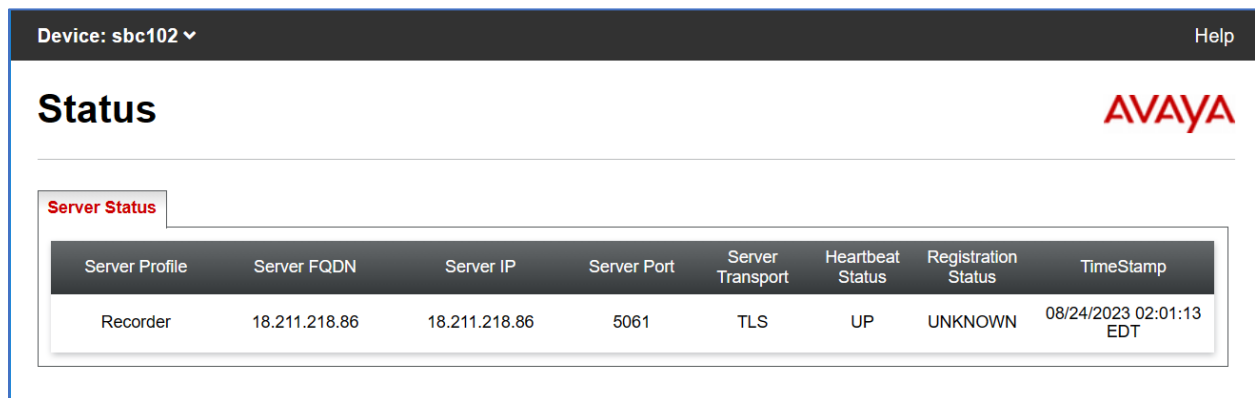
For configuring TLS, the certificate authority (CA) of System Manager is used to create the certificate for the Cogito SIP recording server.

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 SBC

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



Device: sbc102 ▾								Help
Status								AVAYA
Server Status								
Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp	
Recorder	18.211.218.86	18.211.218.86	5061	TLS	UP	UNKNOWN	08/24/2023 02:01:13 EDT	

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 'Status | Status and Control | TSAPI Service Summary' page. The left sidebar lists various services, with 'Status and Control' expanded to show 'TSAPI Service Summary'. The main content area displays 'TSAPI Link Details' with a table of 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	cm10	2	Talking	Sat Jul 15 06:30:50 2023	Online	20	4	15	15	30

Below the table are buttons for 'Online' and 'Offline'. A note states: 'For service-wide information, choose one of the following: TSAPI Service Status | TLink Status | User Status'.

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 username with the time of the connection established.

The screenshot shows the 'Status | Status and Control | TSAPI Service Summary' page with 'User Status' selected. The main content area displays 'CTI User Status' with a table of open streams.

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Sat 15 Jul 2023 06:32:05 AM EDT		AVAYA#CM10#CSTA#AES50
DMCCLCSUserDoNotModify	Sat 15 Jul 2023 06:32:05 AM EDT		AVAYA#CM10#CSTA#AES50
cogito	Tue 22 Aug 2023 02:34:29 AM EDT		AVAYA#CM10#CSTA#AES50

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 Services using 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	
		CTI		CTI		CTI		CTI	
Station Ext		Lnk CRV		Lnk CRV		Lnk CRV		Lnk CRV	
3301		2	0007						
3302		2	0006						
3401		2	0008						
3402		2	0005						

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.

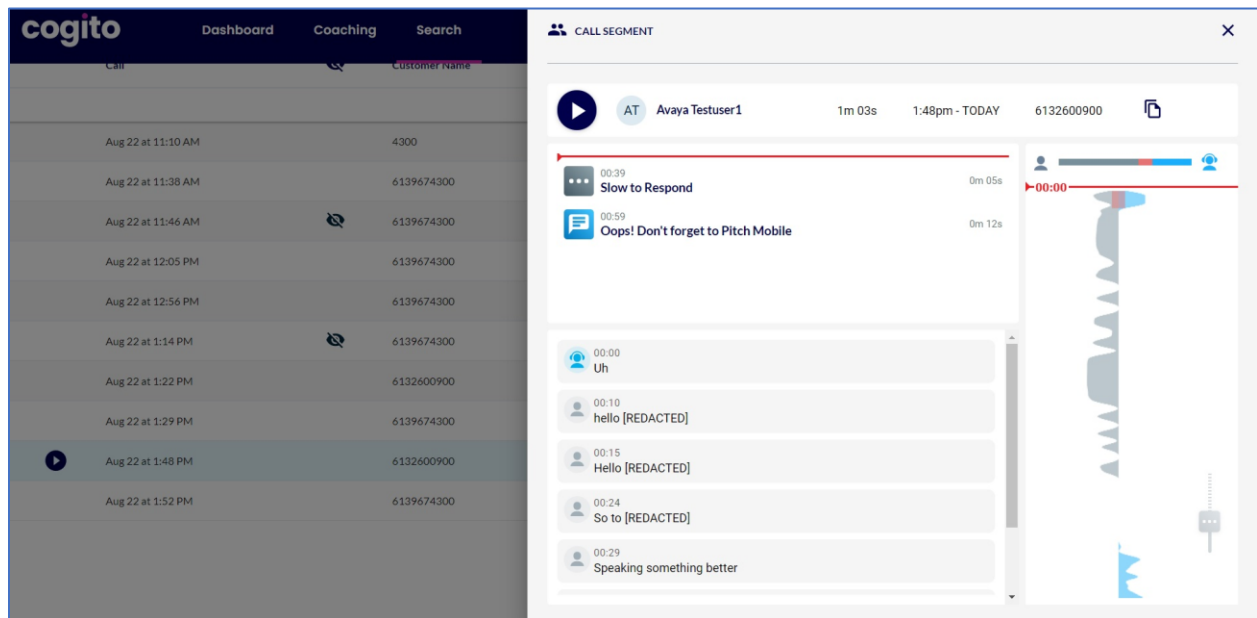
```
list agent-loginID
```

AGENT LOGINID									
Login ID	Name		Extension		Dir	Agt	AAS/AUD		COR
	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv			Skil/Lv	Skil/Lv	
1000	Agent	1000	3301						1
	1/01	/	/	/	/	/	/	/	lv1
1001	Agent	1001	3401						1
	1/01	/	/	/	/	/	/	/	lv1
1002	Agent	1002	3402						1
									lv1

9.4. Verify SIPREC

The steps to verify SIPREC are:

1. Place a call from PSTN to contact center queue via the SIP trunk through the Avaya SBC 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 SBC as shown in the screen below.



4. Disconnect the contact center call from the PSTN user. Verify the Avaya SBC 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 Emotion AI to successfully interoperate with Avaya Aura® Application Enablement Services and Avaya Session Border Controller. 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 10.1, August 2023
- [2] *Deploying Avaya Aura® Communication Manager*, Release 10.1, June 2023
- [3] *Administering Avaya Aura® Communication Manager*, Release 10.1, June 2023
- [4] *Deploying Avaya Aura® Session Manager*, Release 10.1 February 2023
- [5] *Upgrading Avaya Aura® Session Manager* Release 10.1, February 2023
- [6] *Administering Avaya Aura® Session Manager* Release 10.1, February 2023
- [7] *Deploying Avaya Session Border Controller e Release 10.1*, September 2023
- [8] *Upgrading Avaya Session Border Controller Release 10.1*, September 2023
- [9] *Administering Avaya Session Border Controller Release 10.1*, September 2023

©2023 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.