



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Komutel Komlog Release 1.19.1 with Avaya Session Border Controller for Enterprise Release 8.1 Via SIPREC - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Komutel Komlog to interoperate with Avaya Session Border Controller for Enterprise. Komutel Komlog 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 Komutel Komlog to interoperate with Avaya Session Border Controller for Enterprise (Avaya SBCE). Komutel Komlog is a SIPREC call recording solution for emergency 911 calls as well as regular SIP trunk calls through Avaya Session Border Controller for Enterprise.

In the compliance testing, a simulated 911 call generator was used to generate emergency calls that contain specific headers such as GeoLocation, Call-Info...etc. the Komutel Komlog was able to capture the media of the emergency 911 and regular calls with PSTN customers through the SIP trunking service in Avaya Session Border Controller for SIPREC call recording.

2. General Test Approach and Test Results

The general test approach was to verify the features and serviceability of the Komutel Komlog successfully integrate with the Avaya SBCE for call recording via SIPREC.

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 Komutel recording server did not include the use of any specific encryption features.

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.

For the testing associated with these Application Notes, the interface between Avaya systems and the Komutel Komlog did not include use of any specific encryption features as requested by Komutel.

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.

- 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.
- Serviceability testing – The behavior of Komutel recording server under different failure conditions.

Note - The 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 Komutel recording solution was completed successfully with the exception of the observations or limitations described below.

- The Komutel Komlog records an abandoned call that contains the ring back tone on the telephone of the caller as well as the background noise. The reason might be the Komlog starts recording as soon as it was sending back the 200 OK for the INVITE message from the Avaya SBCE and did not wait for the UPDATE message to start recording. This behavior does not impact the regular recording, but it is listed here for reference so that customer is aware of this behavior.
- The Komutel Komlog does not have a feature to show the live recording. It shows the saved recordings and they can be played back from the web portal.
- The Komutel Komlog does not indicate which stream belongs to which party of the call. It simply shows two streams of the call in the player window.

2.3. Support

Technical support on Komutel Komlog can be obtained through the following:

- Phone: (877) 225-9988
- Email: info@komutel.com
- Website: <https://www.komutel.com/en/products/voice-and-data-recording/>

3. Reference Configuration

The **Figure 1** below illustrates the test configuration diagram for the compliance test. In the test diagram, two SIP trunks were configured in the Avaya SBCE to connect to a SIP Service Provider and a simulated 911 emergency CallTester application. The Komutel Komlog recording server solution established a SIP connection to Avaya internal interface A1 to receive SIP messages and audio call recording.

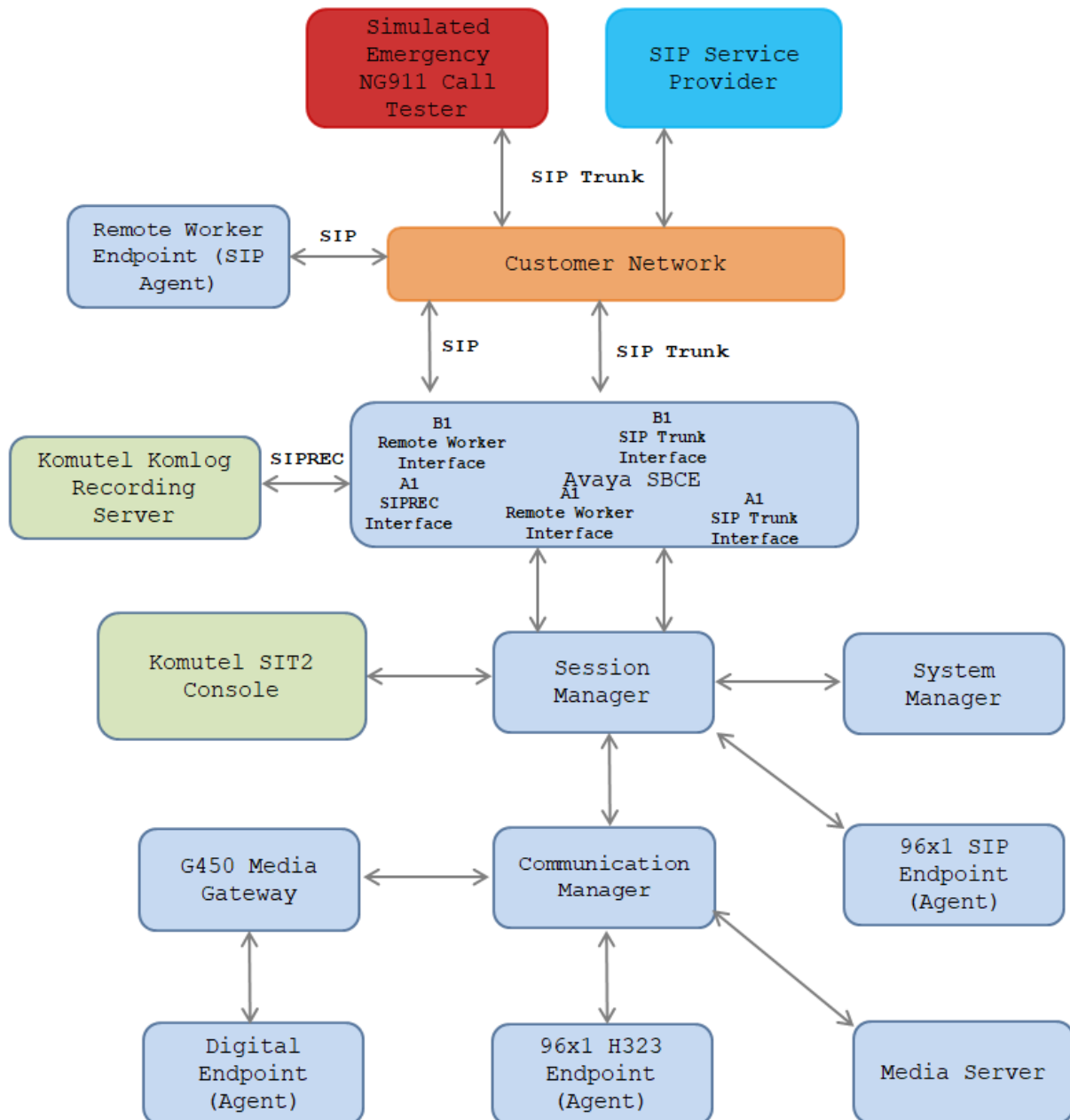


Figure 1 Test Configuration Diagram

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
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
Komutel Komlog recording server	10.33.1.60
Komutel 911 emergency Call Test	10.80.207.89

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 in Virtual Environment	Release 8.1.3 R018x.01.0.890.0 CM 8.1.3.0.0.890.26568
Avaya Aura® System Manager running in Virtual Environment	Release 8.1.3 Build No. - 8.1.0.0.733078 Software Update Revision No: 8.1.3.0.1011784 Feature Pack 3
Avaya Aura® Session Manager running in Virtual Environment	Release 8.1.3 8.1.3.0.813014
Avaya Session Border Controller for Enterprise	8.1.1.0
Avaya Aura® Media Server running on Virtualized Environment	8.0.1.121_2019.04.29
Avaya G450 Media Gateway	41.20.0
Avaya 96x1 IP Deskphones	6.8304 (H.323) 7.1.9.0.8 (SIP)
Avaya 9408 Digital Deskphone	2.0 SP8 (R20)
Komutel Komlog Recording Server running on Windows 2016	1.19.1

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager.

5.1. Administer System Parameters Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the Eir SIP Trunk network, and any other SIP trunks used.

display system-parameters customer-options		Page	2 of
11			
	OPTIONAL FEATURES		
IP PORT CAPACITIES		USED	
	Maximum Administered H.323 Trunks:	12000	0
	Maximum Concurrently Registered IP Stations:	18000	3
	Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
	Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
	Maximum Video Capable Stations:	41000	0
	Maximum Video Capable IP Softphones:	18000	0
	Maximum Administered SIP Trunks:	24000	10
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
	Maximum TN2501 VAL Boards:	128	0
	Maximum Media Gateway VAL Sources:	250	1
	Maximum TN2602 Boards with 80 VoIP Channels:	128	0
	Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:		300	0

Verify **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

```

5.2. Administer Hunt Group

This section provides the Hunt Group configuration for the call center agents. Agents will log into 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 5.7**.

```

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
        Security Code:                                MM Early Answer? n
        ISDN/SIP Caller Display:                      Local Agent Preference? n

        Queue Limit: unlimited
        Calls Warning Threshold:      Port:
        Time Warning Threshold:      Port:

SIP URI:

```


5.3. Administer Vector

Use the command “**change vector n**” while “n” is the vector number. The example of the vector 1 with the basic scripting is shown below. The vector 1 is used for the configuration of then 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						

5.4. 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 5.4** 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*:			

5.5. 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:		

5.6. Configure SIP Trunk

Use the command “**change trunk-group n**” while “n” is number of the trunk group that is previously configured to connect to Avaya Aura® Session Manager. 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 UII: 8	

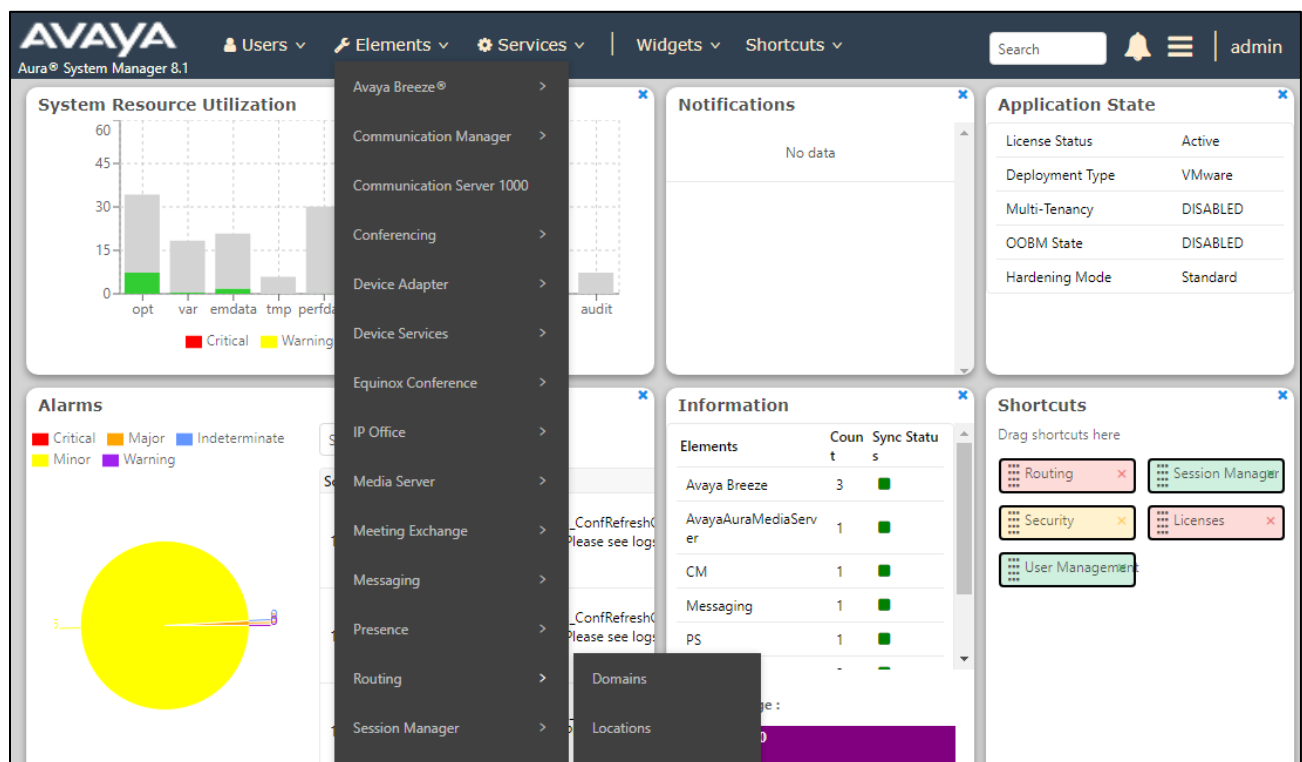
6. Configure Avaya Aura® Session Manager

The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

Note – For the completion of configuring routing in Session Manager for interworking with Communication Manager and the Avaya SBCE please refer to the document in **Section 11** for more detail. This section only mentions about the configuration of the emergency 911 dial pattern in Session Manager.

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed; under **Elements** select **Routing** → **Domains**.



6.2. Emergency Dial Pattern

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, the emergency 911 dial patterns was created to route calls from the simulated 911 system to Communication Manager through Session Manager. Dial Patterns define which routing policy

will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call, for example in this case is 911.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **Emergency Call:** is checked to enable the emergency for this dial pattern.
- **Emergency Priority:** Enter 1 in the box.
- **Emergency Type:** Enter 1 in the box.
- **SIP Domain:** Enter the destination domain used in the match criteria, or select “ALL” to route incoming calls to all SIP domains.
- **Notes:** Add a brief description (optional).
- In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria and select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select** (not shown). Click Commit to save.

In this sample below, the 911 call is routed to Communication Manager and then the 911 call will be routed to the elite call center and an available agent answers the call.

AVAYA
Aura® System Manager 8.1

Users Elements Services Widgets Shortcuts Search admin

Home Routing

Domains
Locations
Conditions
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns

Dial Pattern Details [Commit] [Cancel] [Help ?]

General

* Pattern: 911

* Min: 3

* Max: 3

Emergency Call: ☒

* Emergency Priority: 1

* Emergency Type: 1

SIP Domain: bwvdev.com

Notes:

Originating Locations and Routing Policies

[Add] [Remove]

1 Item Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-CM-Trunk3	0	<input type="checkbox"/>	ACM-Trunk3-Public	Public SIP Trunk

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.

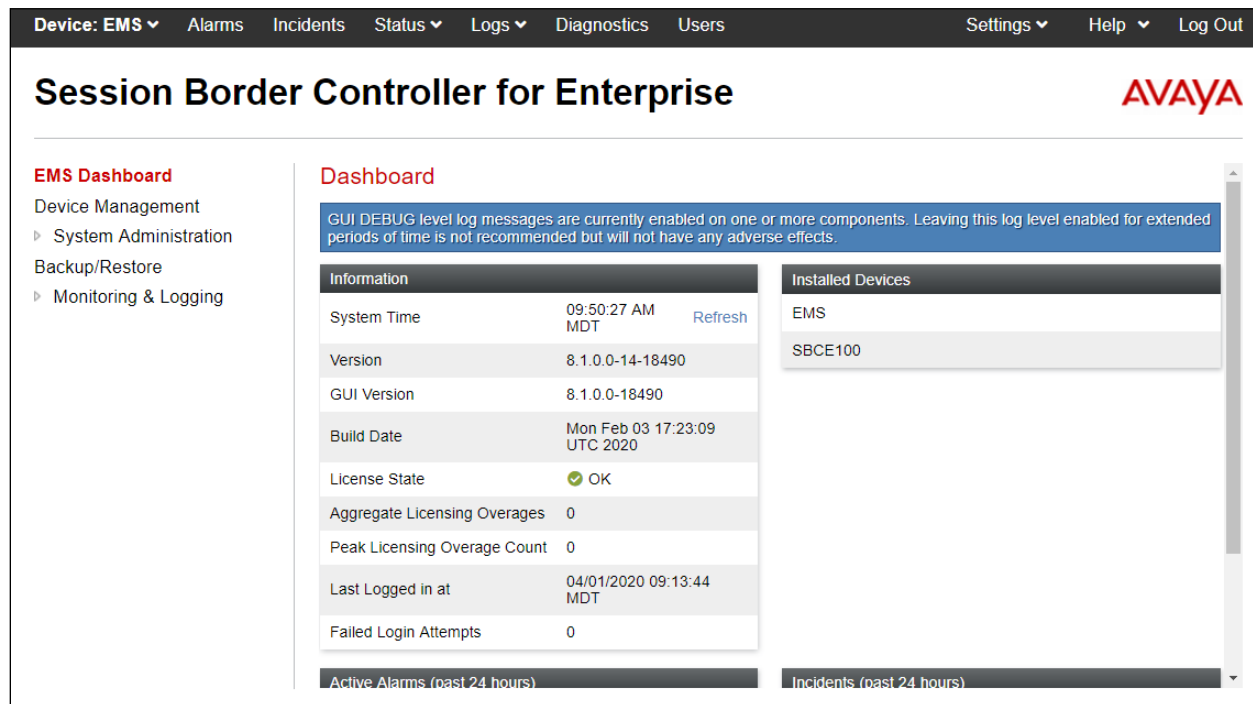
7.1. Access the Management Interface

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, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, there is a "Log In" section. It includes a "Username:" label with a text input field containing "ucsec", and a "Password:" label with a password input field showing masked characters. Below these fields is a "Log In" button. Underneath the button, 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." Below the disclaimer is a 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, there is a copyright notice: "© 2011 - 2018 Avaya Inc. All rights reserved."

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.



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

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

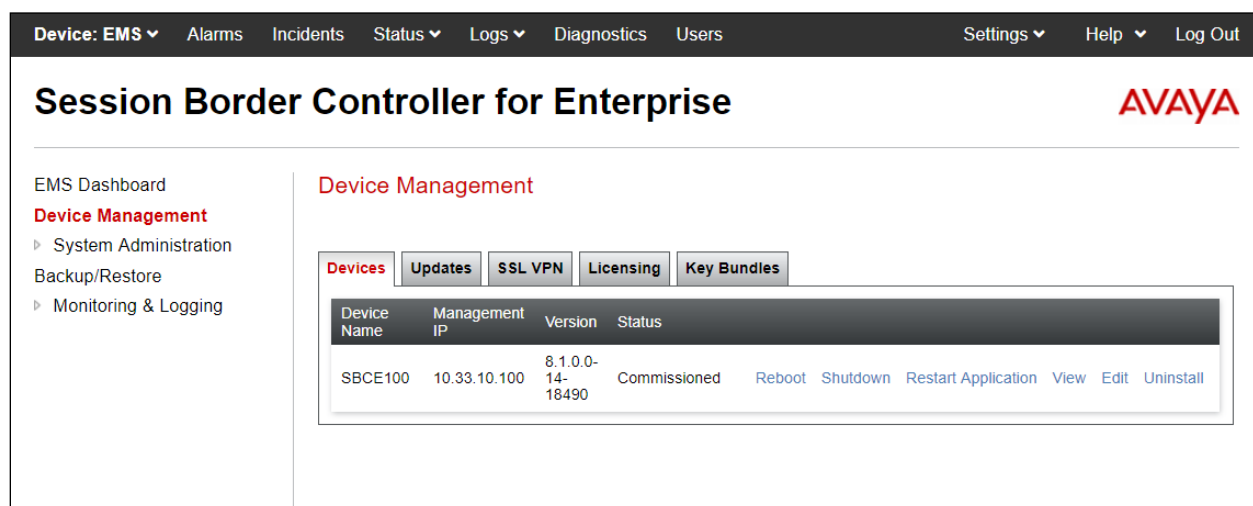
Installed Devices

- 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** highlighted below.



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

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. In 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
X

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	<input checked="" type="checkbox"/>
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
--------------	--------------

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.

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 contains a menu with 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows' (expanded), 'Network Management' (selected), 'Media Interface', 'Signaling Interface', 'End Point Flows', 'Session Flows', 'Advanced Options', 'DMZ Services', and 'Monitoring & Logging'. The main content area is titled 'Network Management' and features two tabs: 'Interfaces' (selected) and 'Networks'. An 'Add VLAN' button is located in the top right of the interface table. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled).

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

7.3. 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 **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **Signaling IP** 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 UDP or TCP on port 5060.

Edit Signaling Interface X

Name	Private_SIPREC_Sig
IP Address	Private_A1 (A1, VLAN 0) 10.33.1.53
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

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
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 used during the testing to connect to the Komutel recording server resides in the private network.

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

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 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various management options, with 'Signaling Interface' highlighted under the 'Network & Flows' section. The main content area, titled 'Signaling Interface', features a table with the following data:

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
Public_SIPREC_Sig	10.207.80.109 Public_B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete

7.4. 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 interface, set the **Media IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **Media IP** to the IP address associated with the private interface (A1) 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 the value "Private_SIPREC_Med".
- IP Address:** A section with a dropdown menu showing "Private_A1 (A1, VLAN 0)" and a text input field below it containing "10.33.1.53".
- Port Range:** A section with 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 public media interface for SIPREC sends media to the Komutel 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

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

Media Interface

Add

Name	Media IP Network	Port Range		
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
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
Public_SIPREC_Med	10.207.80.109 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

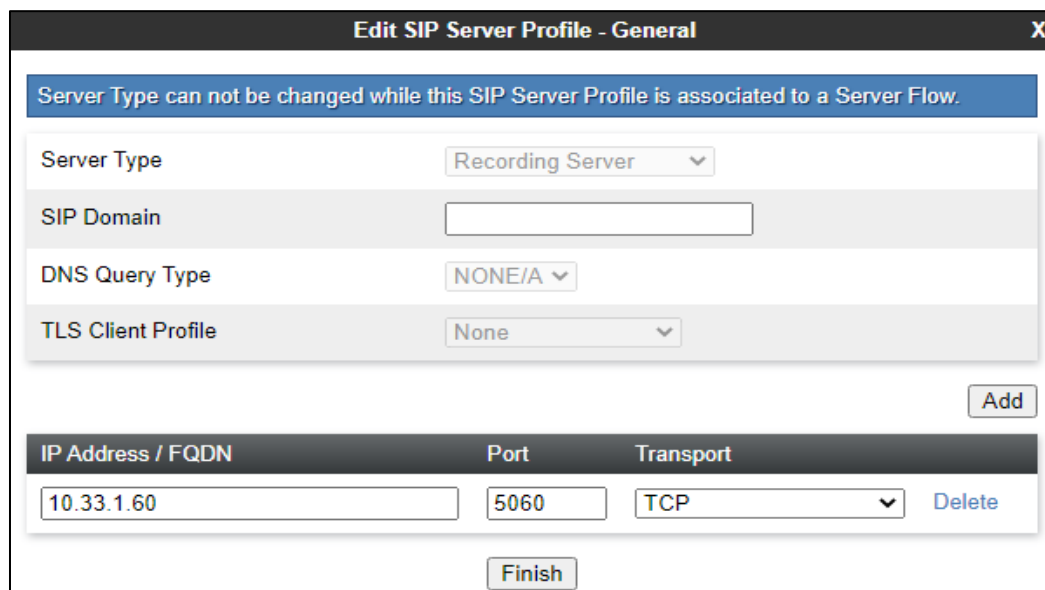
7.5. Server Configuration

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 **Edit SIP Server Profile - General** tab parameters as follow.

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



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 Komutel 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 Komutel.
- **To URI:** enter the uri format as user@ipaddress with the IP address of the Komutel recording server.

Edit SIP Server Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS ▼
Frequency	30 seconds
From URI	ping@10.33.1.53
To URI	ping@10.33.1.60
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**: ☒
- Interworking Profile**:
- Signaling Manipulation Script**:
- Securable**: ☐
- Enable FGDN**: ☐
- TCP Failover Port**:
- TLS Failover Port**:
- Tolerant**: ☐
- URI Group**:

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

7.6. 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 Komutel recording server. The screenshot bellows shows the parameters for the routing profile to Komutel.

- 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:
 - Set **Priority/Weight** to **1**.
 - For **SIP Server Profile**, select **Komlog-Recorder** (Section 7.5) from the pull-down menu. The **Next Hop Address** will be filled-in automatically.
- Keep other parameters as default.

Click **Finish**.

The screenshot shows a configuration window titled "Profile : To-Recorder - Edit Rule". It contains various settings for a routing profile. The "URI Group" is set to "*", "Load Balancing" is set to "Priority", and "Next Hop Priority" is checked. The "Next Hop Address" is set to "10.33.1.60:506". The "SIP Server Profile" is set to "Komlog-". The "ENUM" checkbox is unchecked. The "ENUM Suffix" field is empty. The "Add" button is visible in the bottom right corner. Below the main configuration area, there is a table with columns: "Priority / Weight", "LDAP Search Attribute", "LDAP Search Regex Pattern", "LDAP Search Regex Result", "SIP Server Profile", "Next Hop Address", and "Transport". The table has one row with the following values: "1", an empty field, an empty field, an empty field, "Komlog-", "10.33.1.60:506", and "None". The "Delete" button is visible next to the table row. The "Finish" button is located at the bottom center of the window.

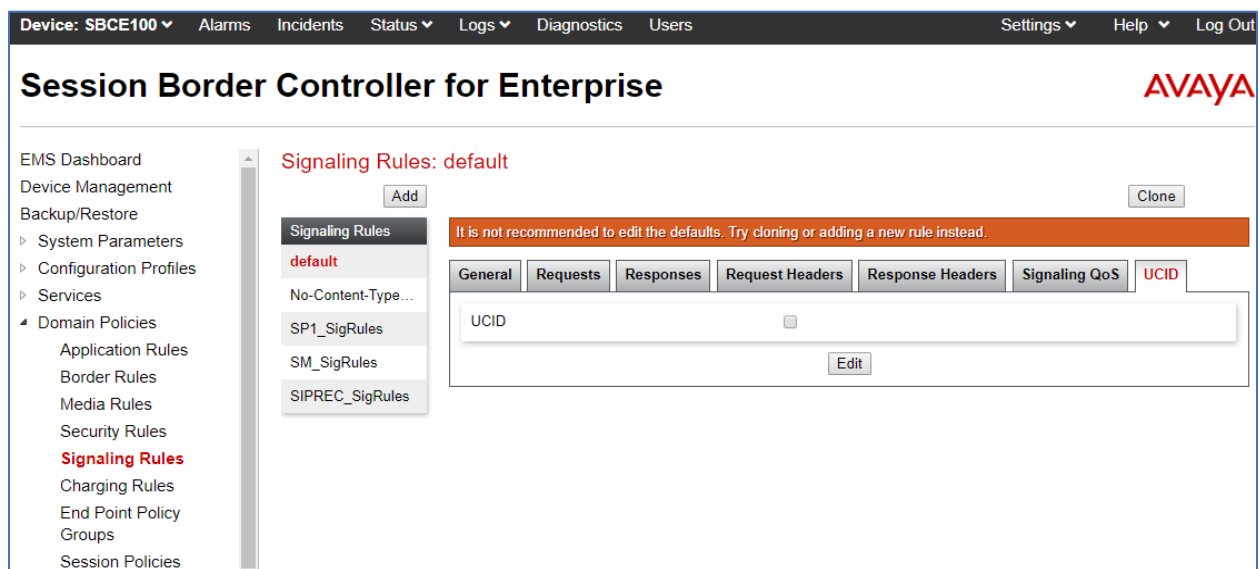
URI Group	Time of Day	Load Balancing	NAPTR	Transport	LDAP Server Profile	LDAP Base DN (Search)	Matched Attribute Priority	Alternate Routing	Next Hop Priority	Next Hop In-Dialog	Ignore Route Header	ENUM	ENUM Suffix
*	default	Priority	<input type="checkbox"/>	None	None	None	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" 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	
1				Komlog-	10.33.1.60:506	None	Delete

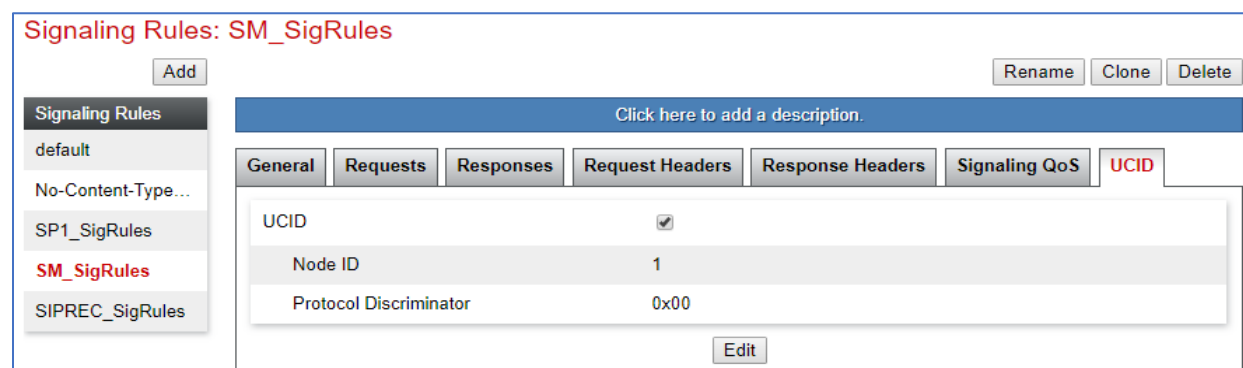
7.7. Signaling Rules

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 Komutel 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 SIP trunk and **SIPREC_SigRules** is created for the Komutel 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 5.7**. The screenshot below shows the signaling rules of Session Manager with UCID enabled.



7.8. 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 Komutel 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 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. The left sidebar lists navigation options: 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 is a table of 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 present for this row. A 'Summary' button is also visible.

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 SIP trunk and **SIPREC_EPG** is created for the Komutel 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 7.7** 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 7.7** 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 Komutel recording server, **SIPREC_EPG**. The policy group uses the **SIPREC_SigRules** created in **Section 7.7** 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

7.9. Recording Profile

To create a new recording profile, navigate to **Configuration Profiles → Recording Profiles** in the left pane. In the center page, select **Add** button (not shown). A pop-up window (not shown) will appear requesting the name of the new group, followed by one of pop-up window in which the routing profile parameters can be configured, select the routing **To-Record** in the **Routing Profile** field and **Full Time** in the **Recording Type** field.

Recording Profile

Call Termination on Recording Failure ☐

Play Recording Tone ☐

Add

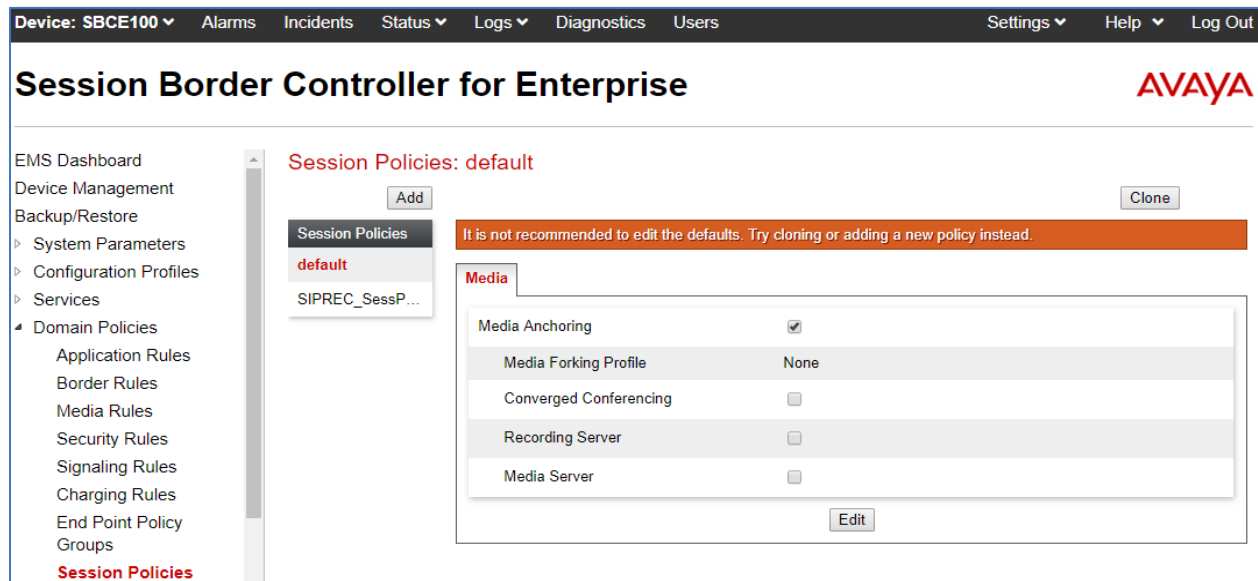
Routing Profile	Recording Type	Video Recording
To-Recorder	Full Time	<input type="checkbox"/>

Delete

Finish

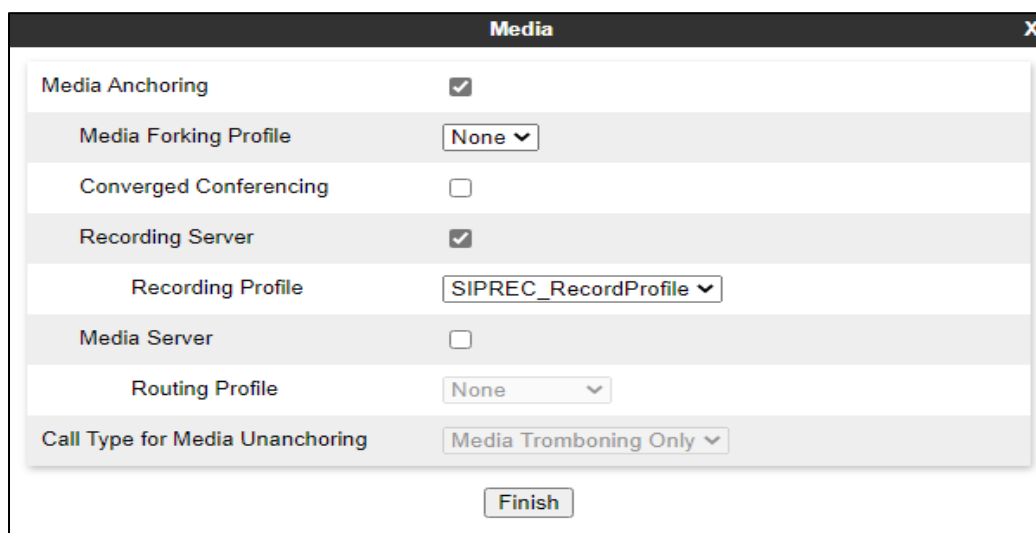
7.10. Session Policies

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.



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

- **Media Anchoring:** checked.
- **Recording Server:** checked.
- **Routing Profile:** select the recording profile *SIPREC_RecordProfile* as configured in **Section 7.9**.



7.11. Session Flows

To create a new session flow, 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 navigation options: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows (selected), Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows (highlighted), Advanced Options, DMZ Services, and Monitoring & Logging. The main content area is titled 'Session Flows' and features an 'Add' button. Below this is a warning message: 'Modifications made to a Session Flow will only take effect on new sessions.' A blue bar with the text 'Click here to add a row description.' is also present. A table lists the 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 with the example "Ex: 192.168.0.1/24" and a single visible option marked with an asterisk (*).
- SBC IP Address (for Subnet #1):** Two dropdown menus, both with a single visible option marked with an asterisk (*).
- Subnet #2:** A text input field with the example "Ex: 192.168.0.1/24" and a single visible option marked with an asterisk (*).
- SBC IP Address (for Subnet #2):** Two dropdown menus, both 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 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.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) 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 reads 'Session Border Controller for Enterprise' with the AVAYA logo. The left sidebar contains a navigation menu with categories like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, and Network & Flows. Under 'Network & Flows', 'End Point Flows' is selected. The main content area is titled 'End Point Flows' and has two tabs: 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active, showing a message: 'Modifications made to a Server Flow will only take effect on new sessions.' Below this is a button to 'Click here to add a row description.' The table below lists four flows for the 'SIP Server: Komlog-Recorder'.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Komlog for SP1 to SM	*	Public1_Sig	Private_SIPREC_Sig	SIPREC_EPG	To-Recorder	View Clone Edit Delete
2	Komlog for SM to SP1	*	Private1_Sig	Private_SIPREC_Sig	SIPREC_EPG	To-Recorder	View Clone Edit Delete
3	Komlog for 911 to SM	*	Public2_Sig	Private_SIPREC_Sig	SIPREC_EPG	To-Recorder	View Clone Edit Delete
4	Komlog for SM to 911	*	Private2_Sig	Private_SIPREC_Sig	SIPREC_EPG	To-Recorder	View Clone Edit Delete

In the testing, there were totally four server flows created for the Komutel recording servers to record calls going through two SIP trunks in Avaya SBCE: one for regular SIP trunk and other for the SIP trunk that simulates the emergency 911.

The screenshot below shows the configuration for the Komutel server flow from the service provider toward the Session Manager, *Komlog for SP1 to SM*:

- **Flow Name:** enter a descriptive name, e.g. **Komlog for SP1 to SM**.
- **SIP Server Profile:** select **Komlog-Recorder** as configured in **Section 7.5**.
- **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 *Private_SIPREC_Sig* as configured in **Section 7.3**.
- **Media Interface:** select *Private_SIPREC_Med* as configured in **Section 7.4**.
- **End Point Policy Group:** select **SIPREC_EPG** as configured in **Section 7.6**.
- **Routing Profile:** select *To-Recorder* as configured in **Section 7.6**.
- Keep other fields at the default values.

Edit Flow: Komlog for SP1 to SM
X

Flow Name	Komlog for SP1 to SM
SIP Server Profile	Komlog-Recorder ▼
URI Group	* ▼
Transport	* ▼
Remote Subnet	*
Received Interface	Public1_Sig ▼
Signaling Interface	Private_SIPREC_Sig ▼
Media Interface	Private_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 Komutel server flow from the Session Manager toward the service provider, **Komlog for SM to SP1**:

- **Flow Name**: enter a descriptive name, e.g. **Komlog for SM to SP1**.
- **SIP Server Profile**: select **Komlog-Recorder** as configured in **Section 7.5**.
- **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 **Private_SIPREC_Sig** as configured in **Section 7.3**.
- **Media Interface**: select **Private_SIPREC_Med** as configured in **Section 7.4**.
- **End Point Policy Group**: select **SIPREC_EPG** as configured in **Section 7.6**.
- **Routing Profile**: select **To-Recorder** as configured in **Section 7.6**.
- Keep other fields at the default values.

Edit Flow: Komlog for SM to SP1	
Flow Name	Komlog for SM to SP1
SIP Server Profile	Komlog-Recorder
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private1_Sig
Signaling Interface	Private_SIPREC_Sig
Media Interface	Private_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 Komutel server flow from the simulated 911 toward the Session Manager, *Komlog for 911 to SM*:

- **Flow Name:** enter a descriptive name, e.g. **Komlog for 911 to SM**.
- **SIP Server Profile:** select **Komlog-Recorder** as configured in **Section 7.5**.
- **Received Interface:** select **Public2_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 **Private_SIPREC_Sig** as configured in **Section 7.3**.
- **Media Interface:** select **Private_SIPREC_Med** as configured in **Section 7.4**.
- **End Point Policy Group:** select **SIPREC_EPG** as configured in **Section 7.6**.
- **Routing Profile:** select **To-Recorder** as configured in **Section 7.6**.
- Keep other fields at the default values.

Edit Flow: Komlog for 911 to SM	
Flow Name	Komlog for 911 to SM
SIP Server Profile	Komlog-Recorder
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public2_Sig
Signaling Interface	Private_SIPREC_Sig
Media Interface	Private_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 Komutel server flow from the Session Manager toward the simulated emergency 911, *Komlog for SM to 911*:

- **Flow Name:** enter a descriptive name, e.g. *Komlog for SM to 911*.
- **SIP Server Profile:** select *Komlog-Recorder* as configured in **Section 7.5**.
- **Received Interface:** select *Private2_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 *Private_SIPREC_Sig* as configured in **Section 7.3**.
- **Media Interface:** select *Private_SIPREC_Med* as configured in **Section 7.4**.
- **End Point Policy Group:** select *SIPREC_EPG* as configured in **Section 7.6**.
- **Routing Profile:** select *To-Recorder* as configured in **Section 7.6**.

Keep other fields at the default values

Edit Flow: Komlog for SM to 911	
Flow Name	Komlog for SM to 911
SIP Server Profile	Komlog-Recorder
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private2_Sig
Signaling Interface	Private_SIPREC_Sig
Media Interface	Private_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	

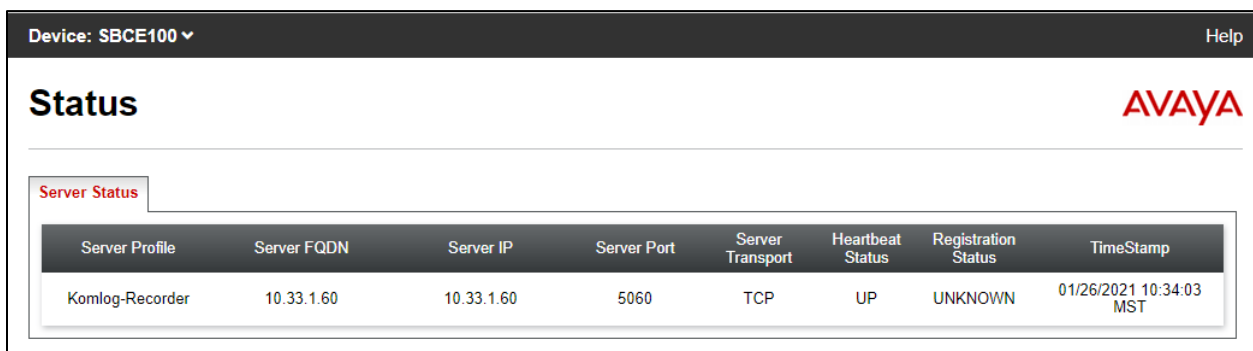
8. Configure Komutel Komlog Recording

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

9. Verification Steps

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

Verify the status of the Komutel 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”.



Device: SBCE100 ▾								Help
Status								AVAYA
Server Status								
Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp	
Komlog-Recorder	10.33.1.60	10.33.1.60	5060	TCP	UP	UNKNOWN	01/26/2021 10:34:03 MST	

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

Verification Steps for SIPREC:

1. Place a call from the simulated 911 call tester to the 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 Komutel recording server receives a live recording call from the Avaya SBCE.

4. Disconnect the contact center call from the PSTN user. Verify the Avaya SBCE sends Bye message to the Komutel recording server and receive responses from Komutel to end the recording call.
5. Verify and play back the recording from the Komlog portal as shown in the screenshot below.

The screenshot displays the Komlog portal interface. At the top, there are tabs for Portal, Charts, Timeline, and Audit log. The Timeline tab is active. On the left, there is a Filters sidebar with options: Since midnight, Last 7 days, Last 30 days, and All recordings. The main area shows a table of recordings for the 'Last 7 days' period. The table has columns for Format, Role, End date/time, Called number, Called name, Caller number, and Length. Below the table, there is a 'Player' section with a waveform and playback controls. The status bar at the bottom indicates 'Tuesday January 26, 1:00:33 PM' and 'KOMUTEL'.

Format	Role	End date/time	Called number	Called name	Caller number	Length
<input checked="" type="checkbox"/>	Phone	1/26/2021, 12:58:26 PM	ASBCE		6139172548, ASBCE	00:55
<input type="checkbox"/>	Phone	1/26/2021, 12:53:42 PM	ASBCE		4234689369, ASBCE	01:07
<input type="checkbox"/>	Phone	1/26/2021, 12:51:58 PM	ASBCE		4234689369, ASBCE	00:06
<input type="checkbox"/>	Phone	1/26/2021, 12:51:25 PM	ASBCE		6132600771, ASBCE	01:00
<input type="checkbox"/>	Phone	1/26/2021, 12:49:14 PM	ASBCE		6132600900, ASBCE	03:09

Page 1 out of 1 | 50 | Recordings 1 - 7 out of 7

Comment

Player

Volume | Rate: 1x

[00:03 / 00:56] ~ 1/26/2021, 12:57:33 PM | Segment 1/1 | Recording: 199

Tuesday January 26, 1:00:33 PM | KOMUTEL

10. Conclusion

These Application Notes describe the configuration steps required for Komutel Komlog recording solution to successfully interoperate with Avaya Session Border Controller for Enterprise. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

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
- [10] Application Notes for Configuring the TELUS SIP Trunking Service IP Authentication on Release 2 Platform with Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0 and Avaya Session Border Controller for Enterprise 7.2 – Issue 1.0
- [11] Application Notes for Configuring Bell Canada SIP Trunk with Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0 and Avaya Session Border Controller for Enterprise 7.2 – Issue 1.0

©2021 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.