Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

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

1. Introduction

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

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

2. General Test Approach and Test Results

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

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

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

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

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

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

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

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

2.1. Interoperability Compliance Testing

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

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

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

2.2. Test Results

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

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

2.3. Support

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

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

3. Reference Configuration

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

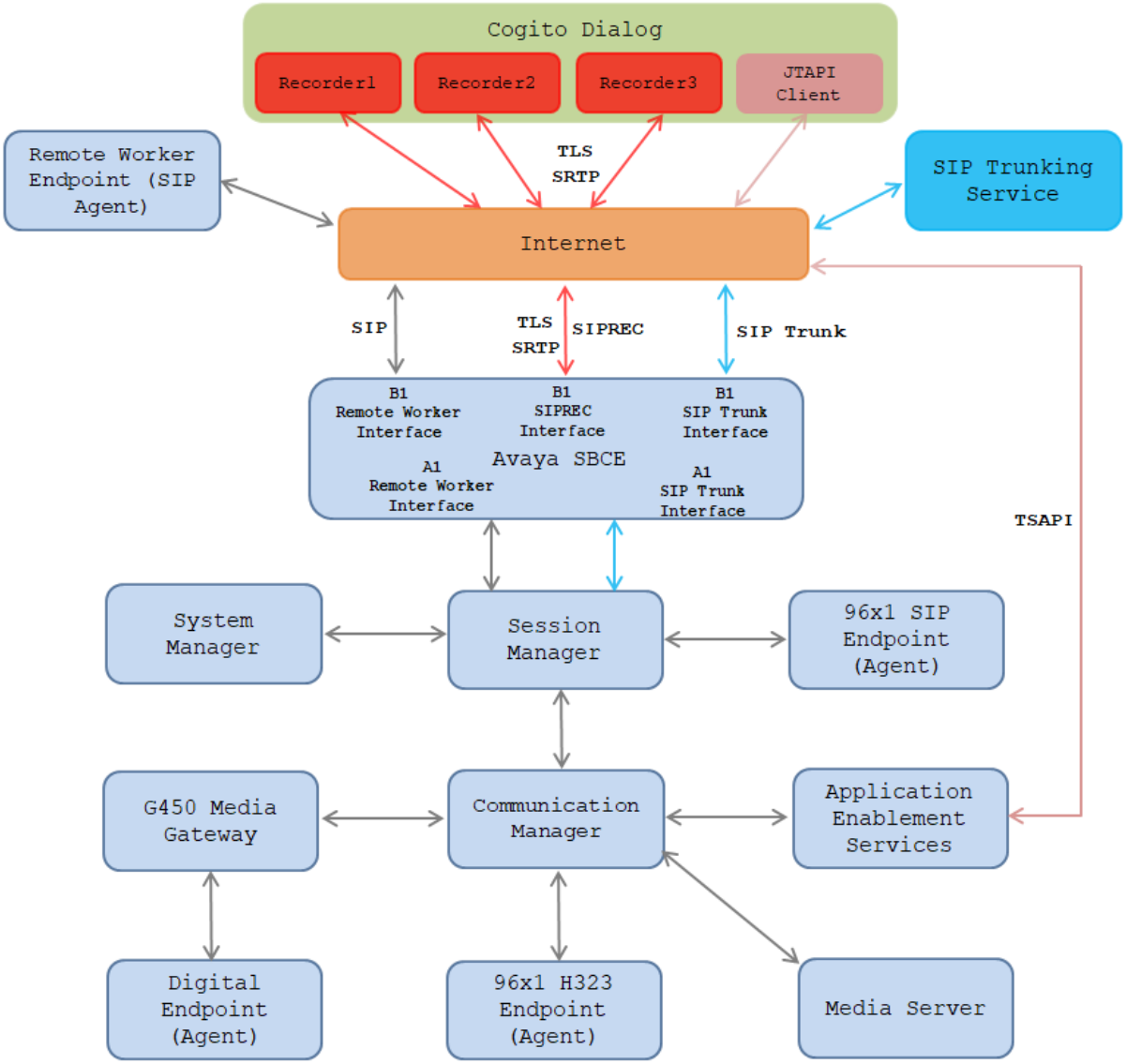


Figure 1 Test Configuration Diagram for Cogito Dialog

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

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

4. Equipment and Software Validated

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

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

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager.

5.1. Verify License

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

```
display system-parameters customer-options                    Page   4 of  12
                                OPTIONAL FEATURES

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

5.2. Administer CTI Link

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

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

5.3. Administer System Parameters Features

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

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

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

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

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

```
change system-parameters features                                 Page  13 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

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

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

5.4. Administer AE Services

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

```
change ip-services                                          Page   1 of
4

                                    IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      procr            8765
```

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

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

```
change ip-services                                          Page   4 of
4
                           AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aes8              *                     y        in use
      2:      aes81             *                     y        in use
```

5.5. Administer Hunt Group

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

```
add hunt-group 1                                                Page   1 of   4
                              HUNT GROUP

            Group Number: 1                                  ACD? y
              Group Name: Skill-1                          Queue? y
         Group Extension: 3320                           Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                     MM Early Answer? n
           Security Code:                Local Agent Preference? n
 ISDN/SIP Caller Display:

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

SIP URI:
```

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

```
add hunt-group 1                                                Page   2 of   4

                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n        Service Level Target (% in sec): 80 in
20
                 Measured: both
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:

   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

5.6. Administer Vector

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

```
change vector 1                                                Page   1 of
6
                                 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 SBCE. Go to **Page 3**, select "***shared***" in the **UUI Treatment** field. With the selection of shared UUI, 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
                                                 UUI Treatment: shared
                                               Maximum Size of UUI 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 UUI 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 UUI: 8
```

6. Configure Avaya Aura® Application Enablement Services

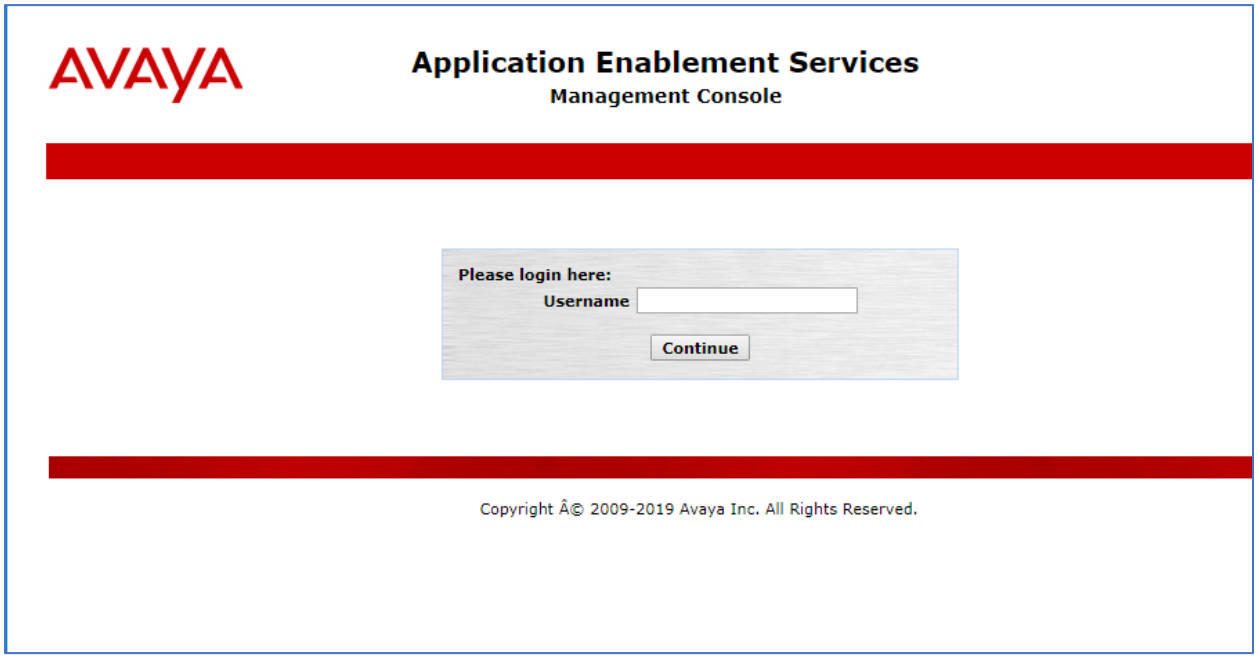
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

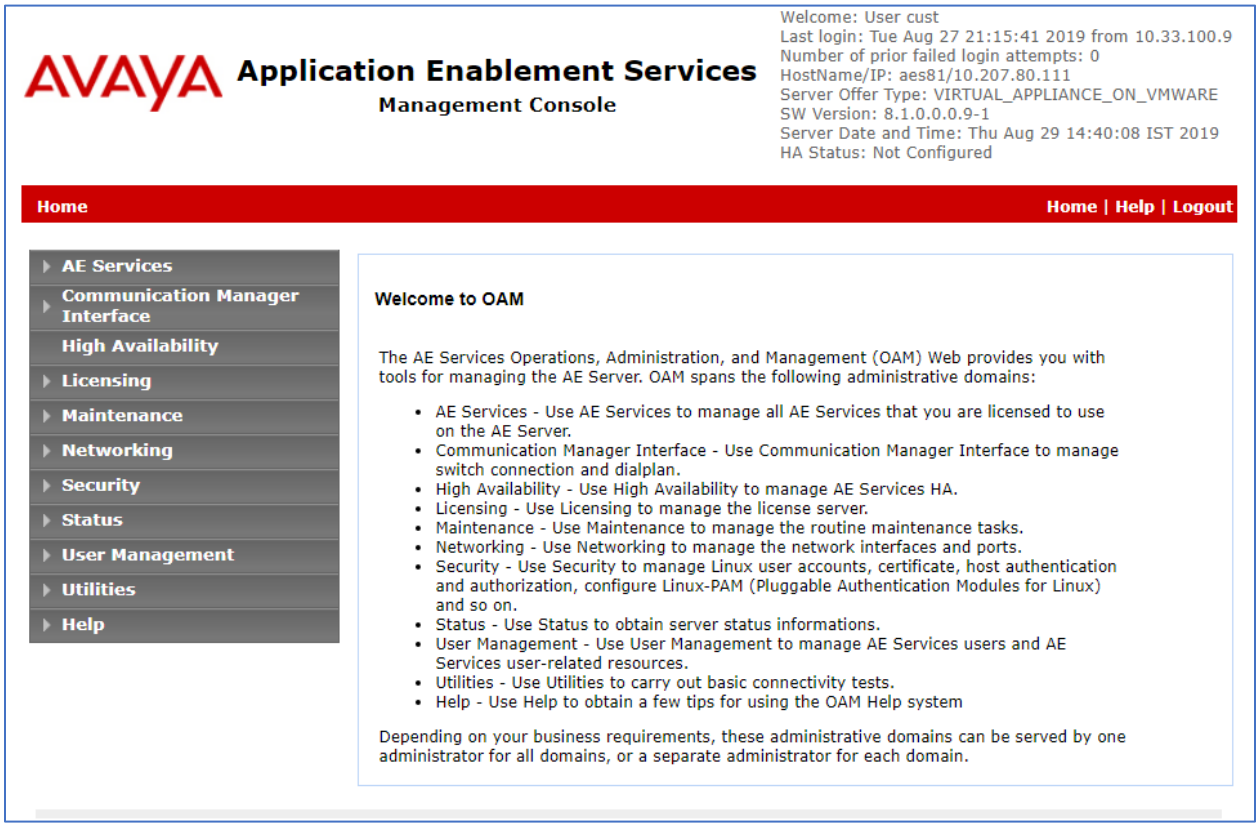
6.1. Launch AE web Interface

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.

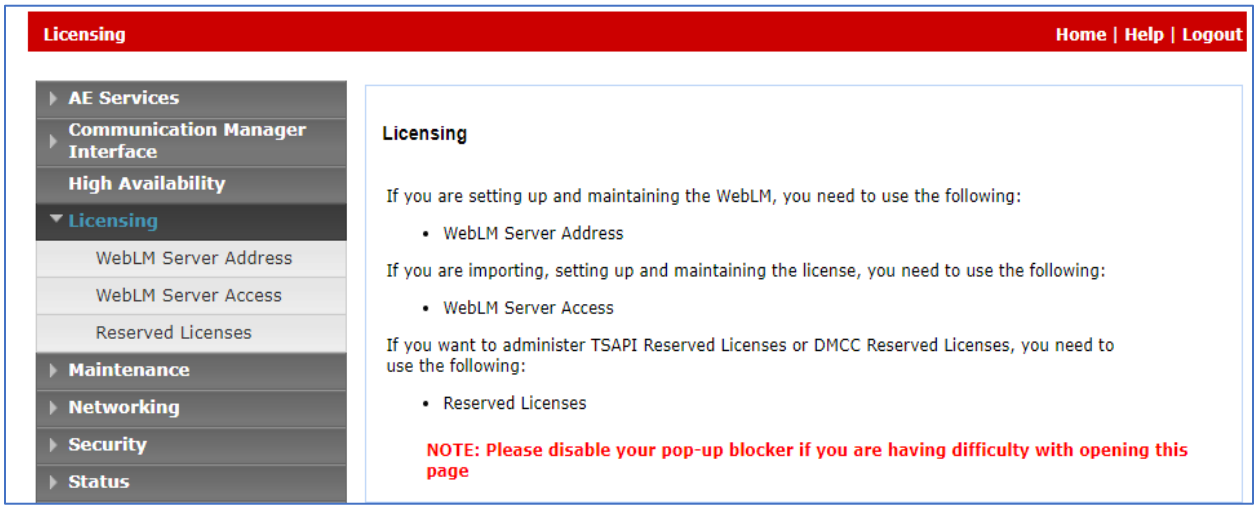


The **Welcome to OAM** screen is displayed next.



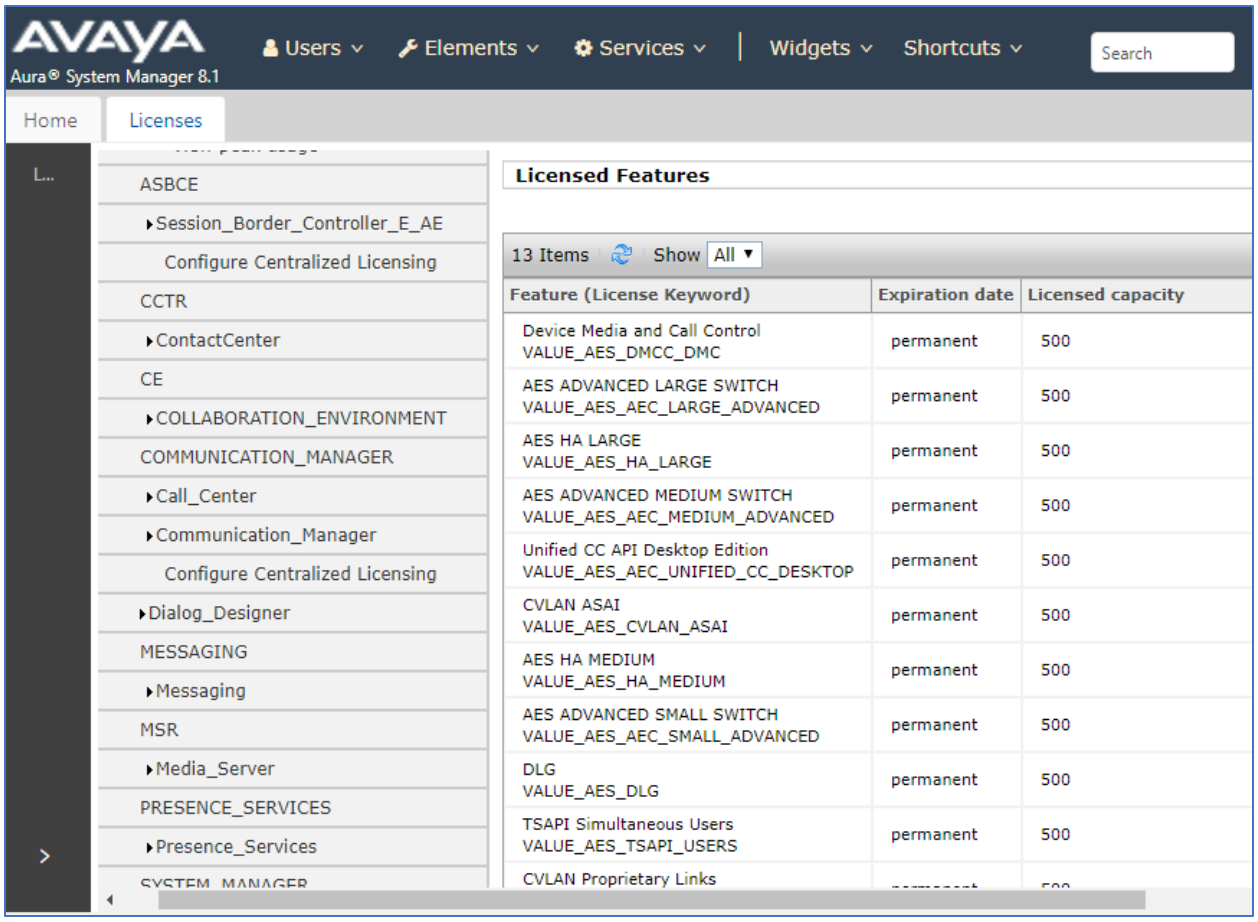
6.2. Verify License

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).



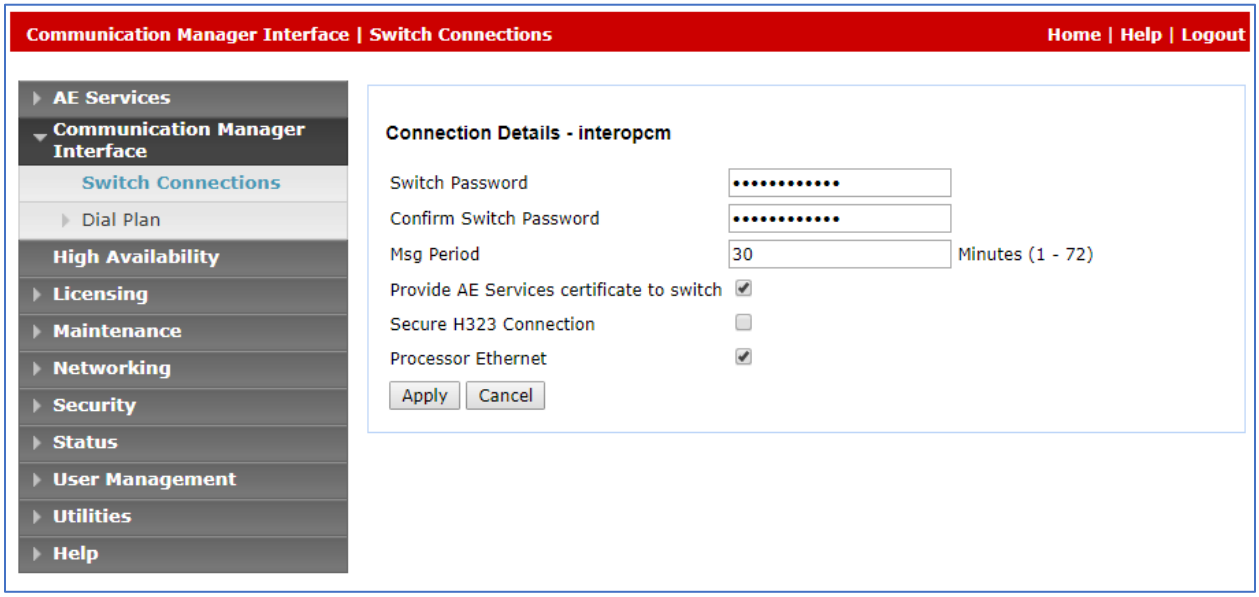
Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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

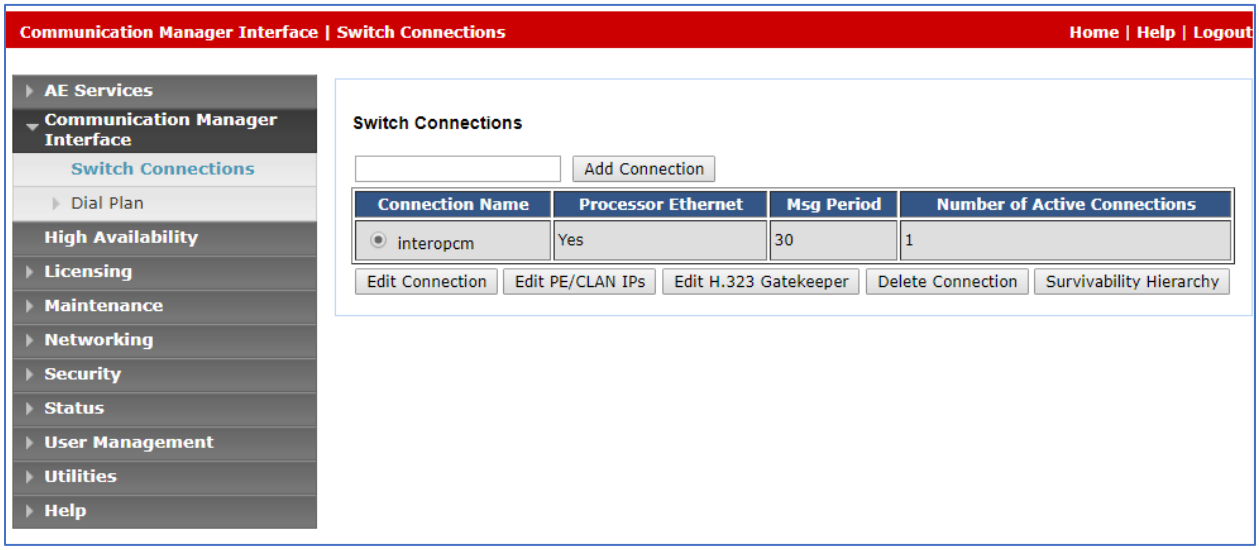


6.3. Administer Switch Connection

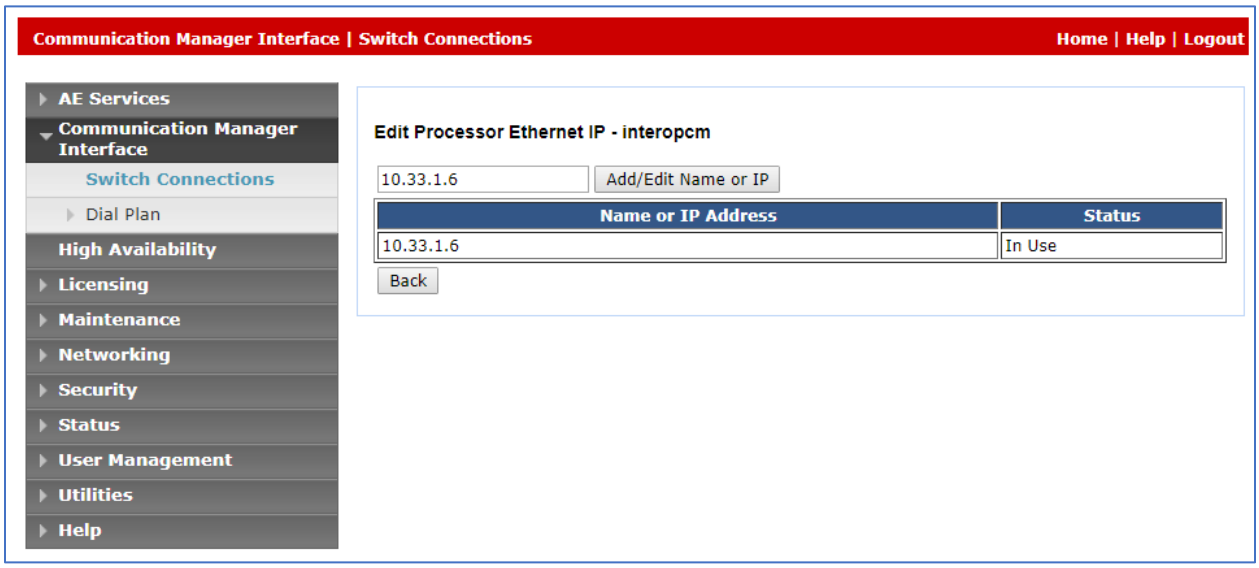
Select **Communication Manager Interface → Switch Connections** from the left pane of the **Management Console**, enter a name in the **Switch Connection** box and click the **Add** button (not shown). Enter the password as configured in **Section 5.4** in the **Switch Password** and **Confirm Switch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



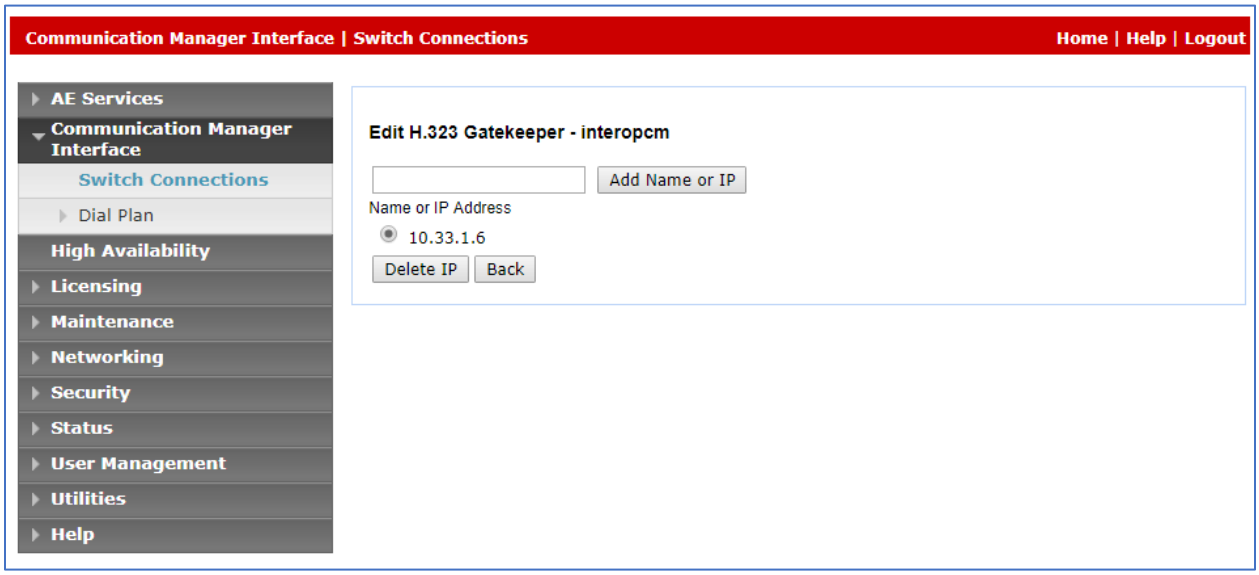
Select the **interopcm** switch connection has been added above and selects **Edit PE/CLAN IPs** to add the IP address of the switch connection.



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.

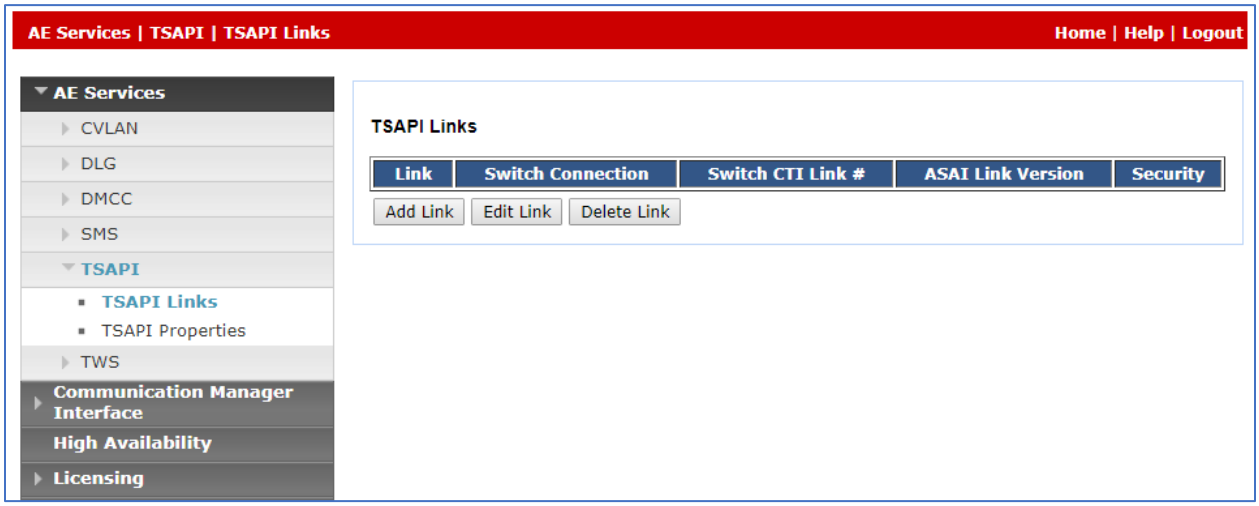


Select the **Edit H.323 Gatekeeper** button to add an IP address of gate keeper, the Gatekeeper IP address in this case is also the Processor Ethernet.

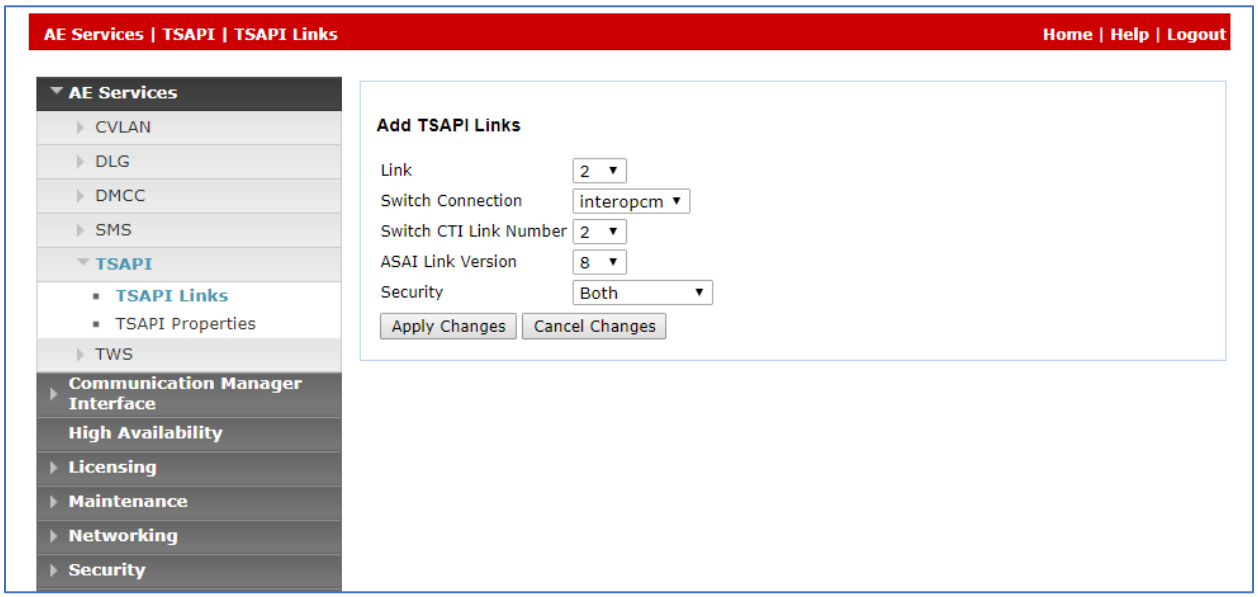


6.4. Administer TSAPI Link

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**.

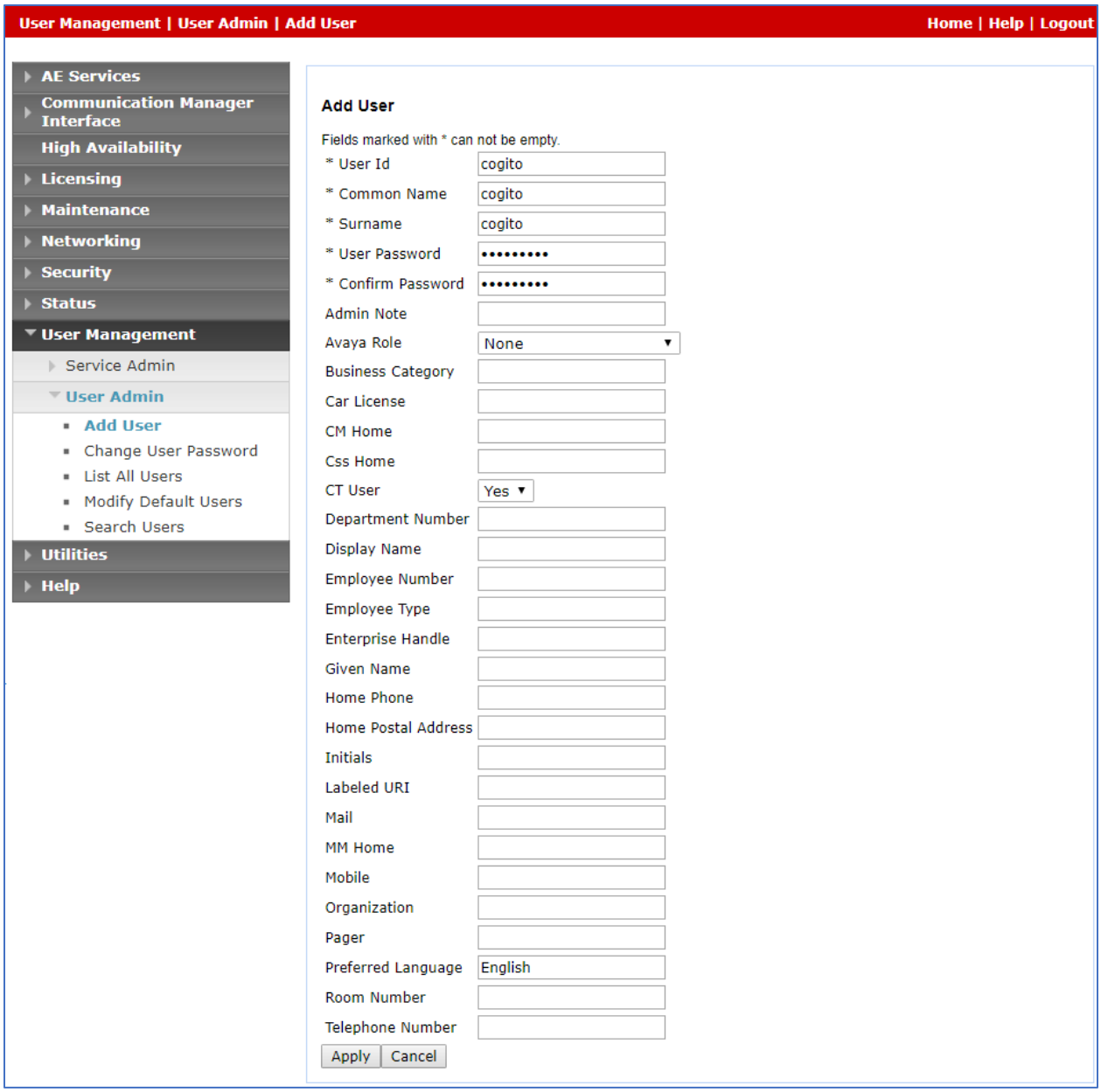


The **Add TSAPI Links** screen is displayed in the right side. The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch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



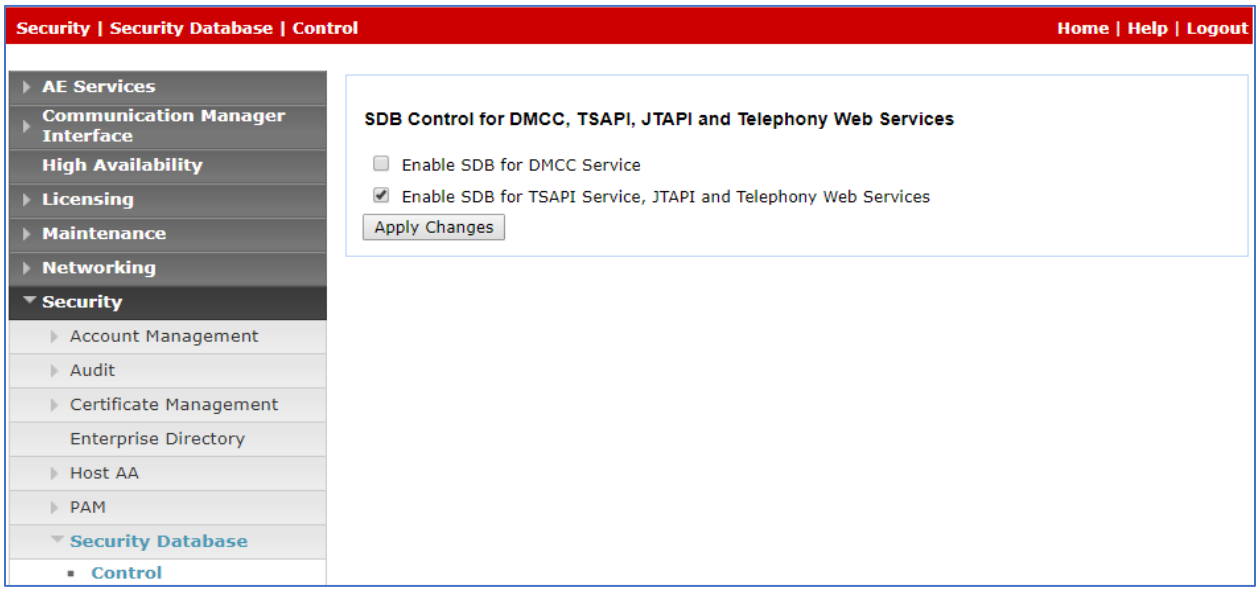
6.5. Administer CTI User

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.

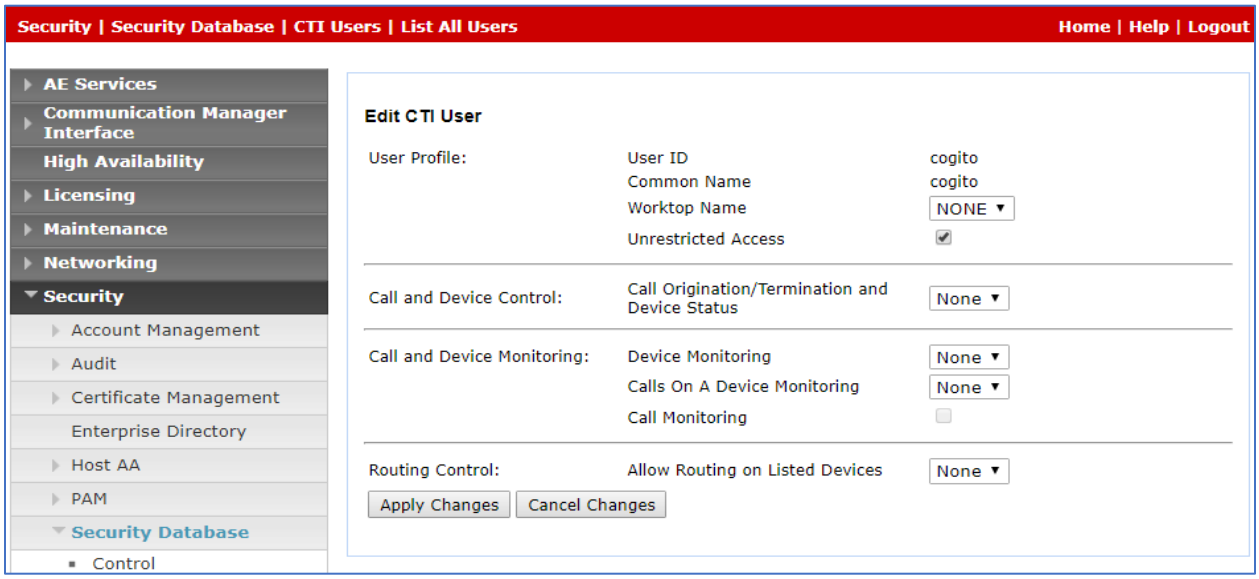


6.6. Configure Security Database

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**.

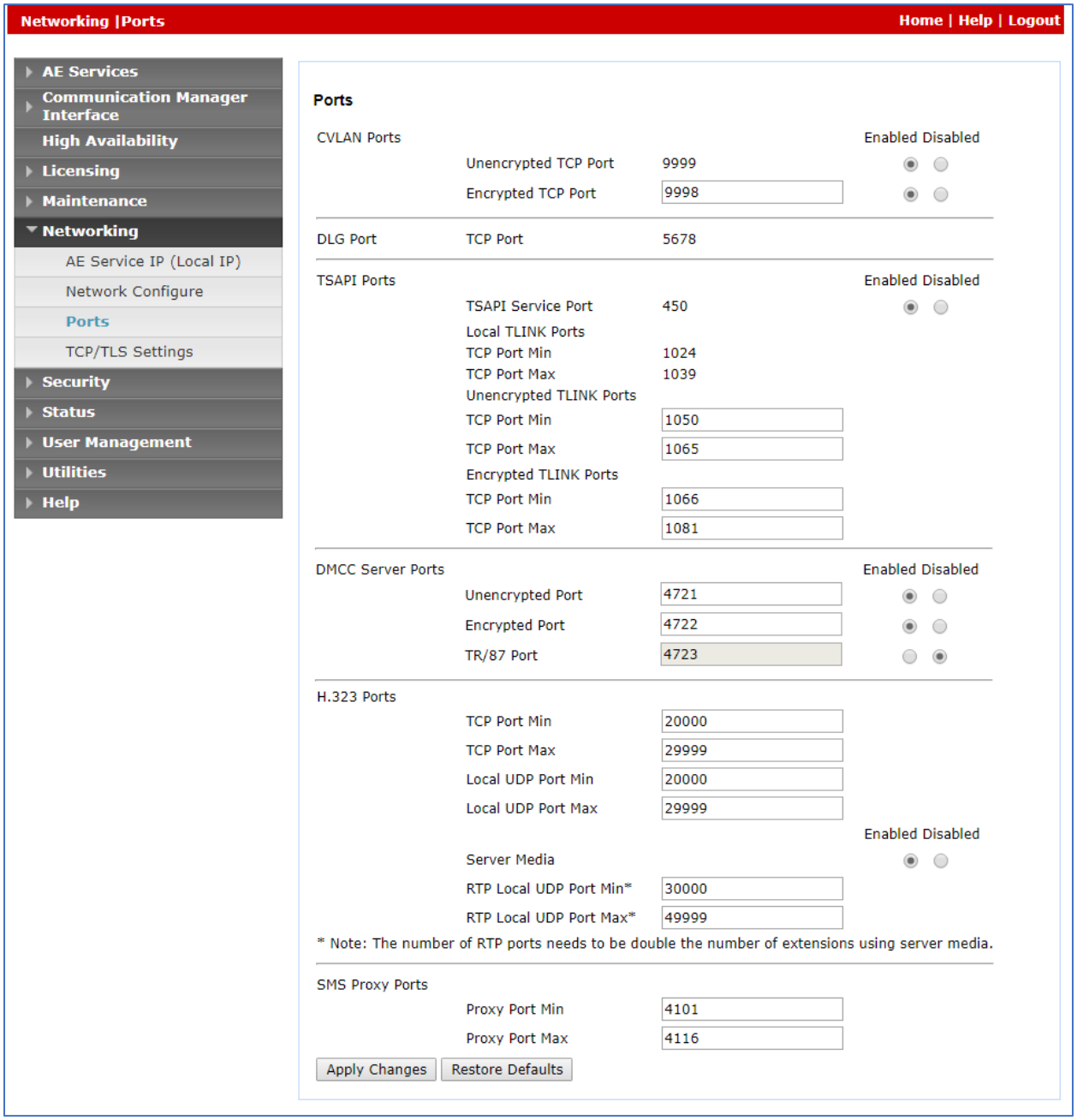


Select **Security → Security Database → CTI Users → List All Users** and select the "cogito" CTI user which is created in **Section 6.5** and select **Edit** button (not shown). In the **Edit CTI User**, select the check box **Unrestricted Access** and click **Apply Changes** to save the configuration.



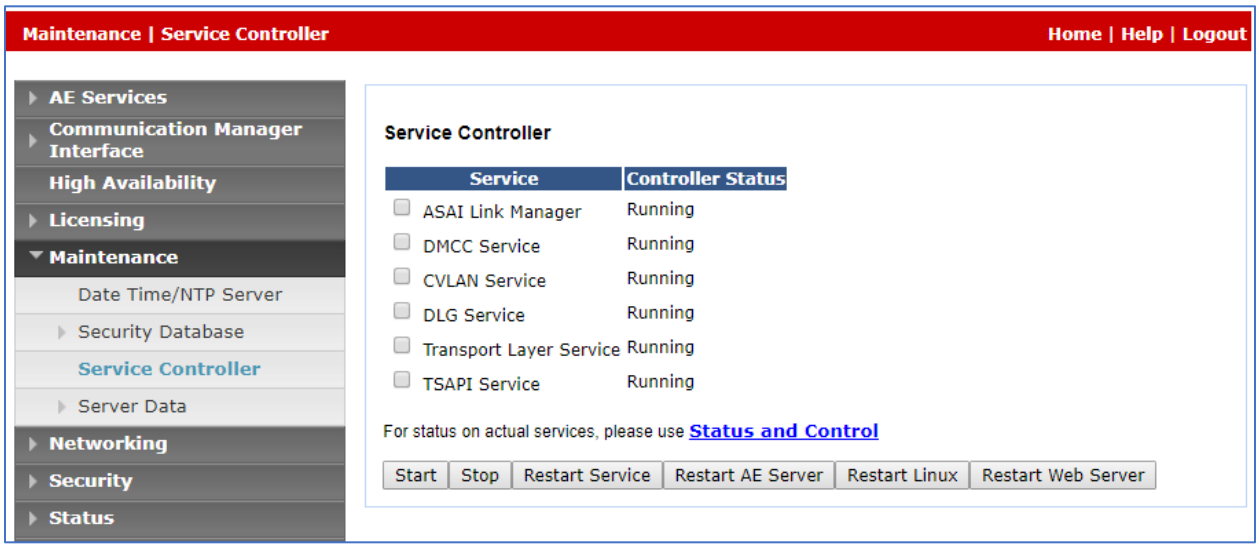
6.7. Administer Ports

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.



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**.



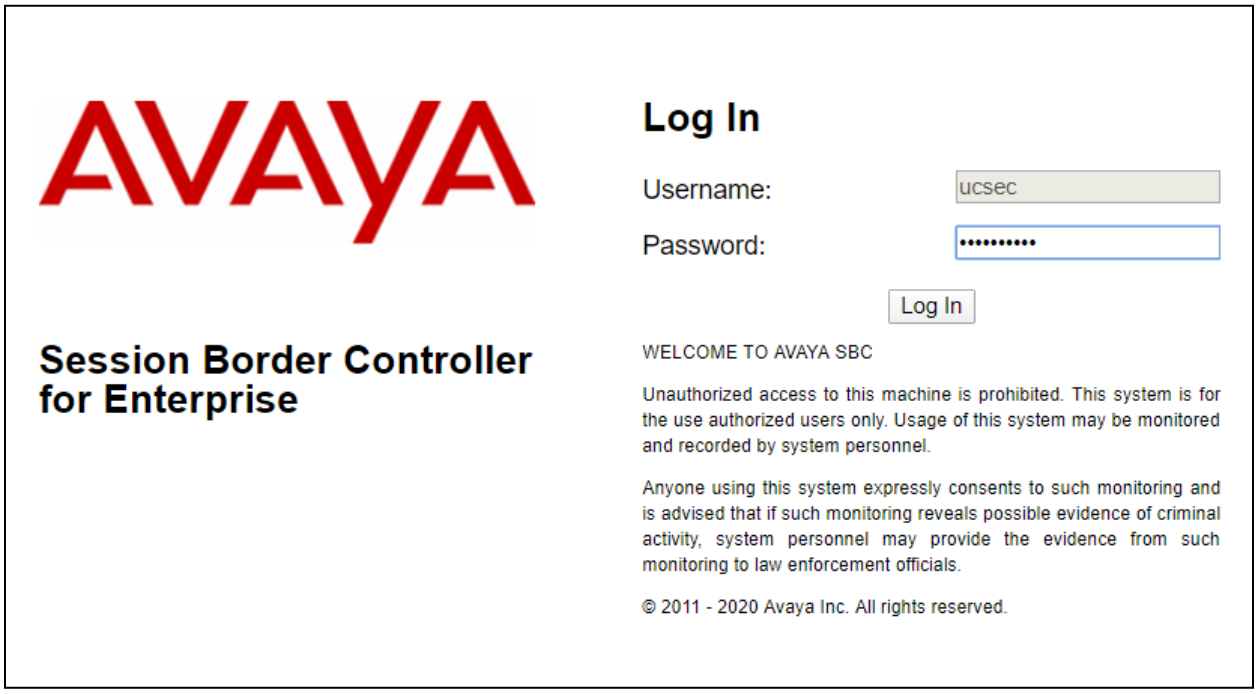
7. Configure Session Border Controller for Enterprise

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).

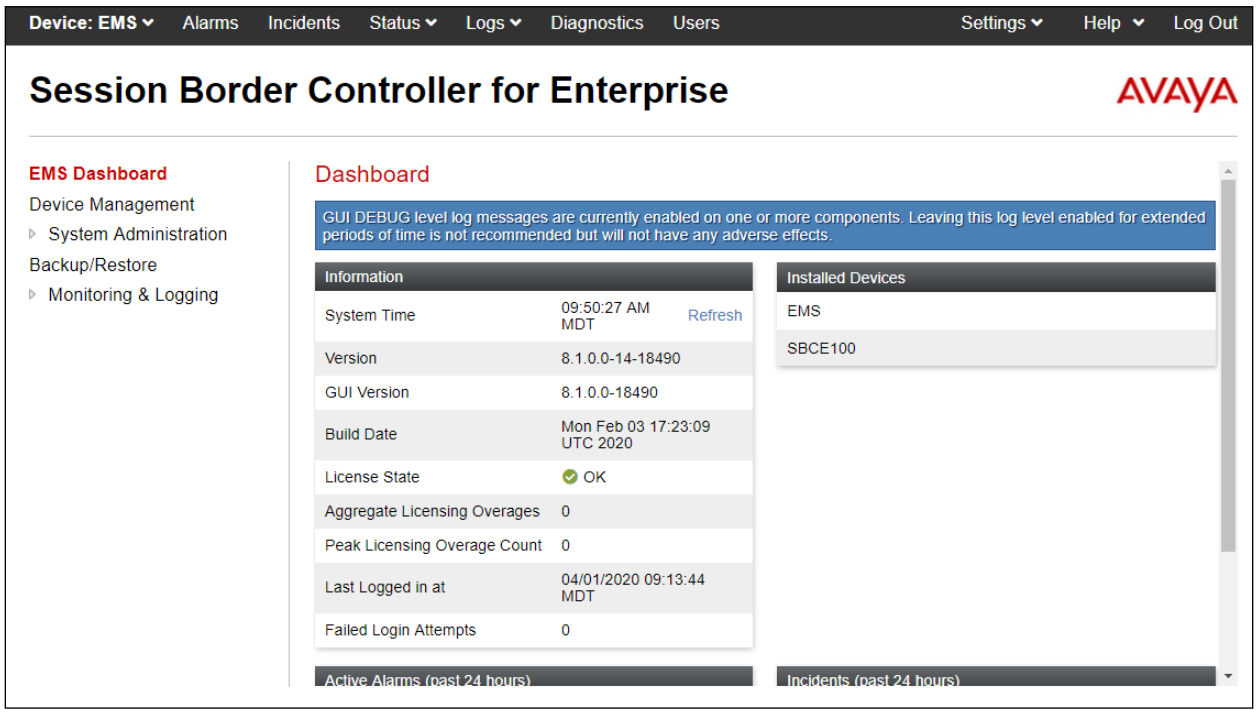
On all screens described in this section, it is assumed that parameters are left at their default values unless specified otherwise.

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.

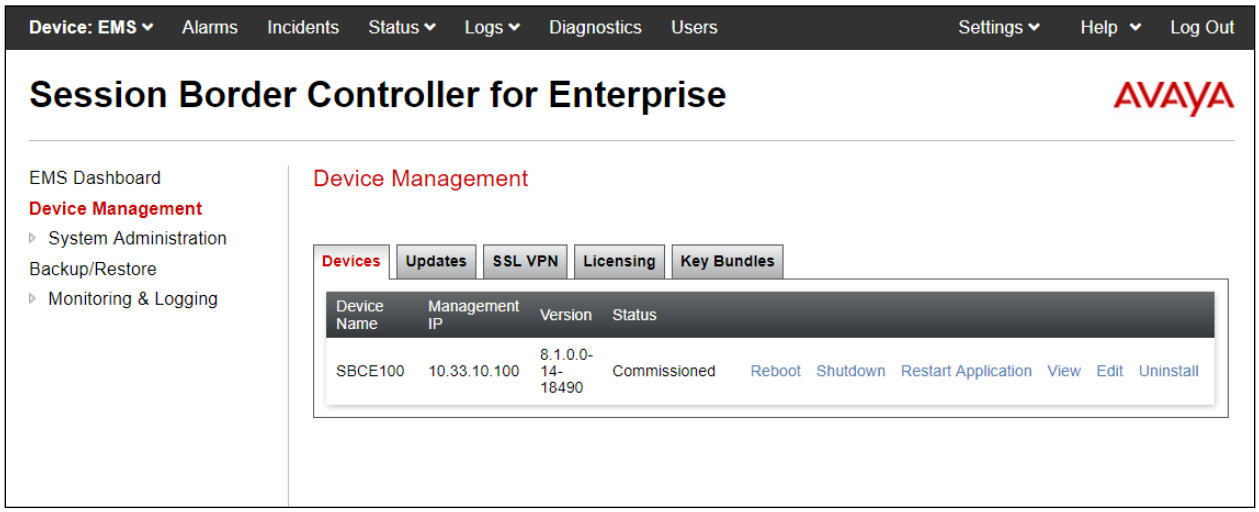


After logging in, the Dashboard screen will appear as shown below. All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

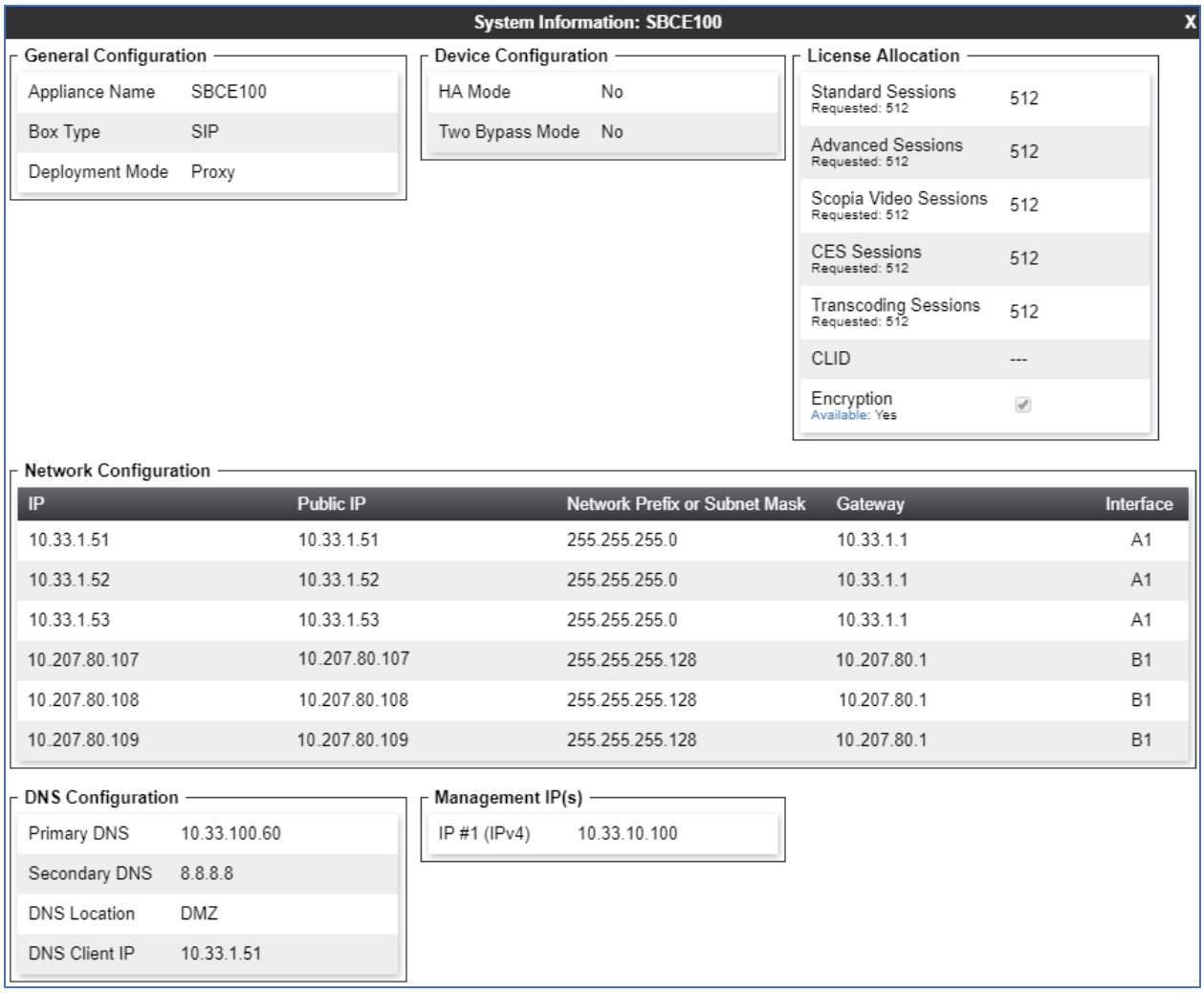


7.2. Verify Network Configuration and Enable Interfaces

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



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



System Information: SBCE100

General Configuration

Appliance Name	SBCE100
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

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

Network Configuration

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

DNS Configuration

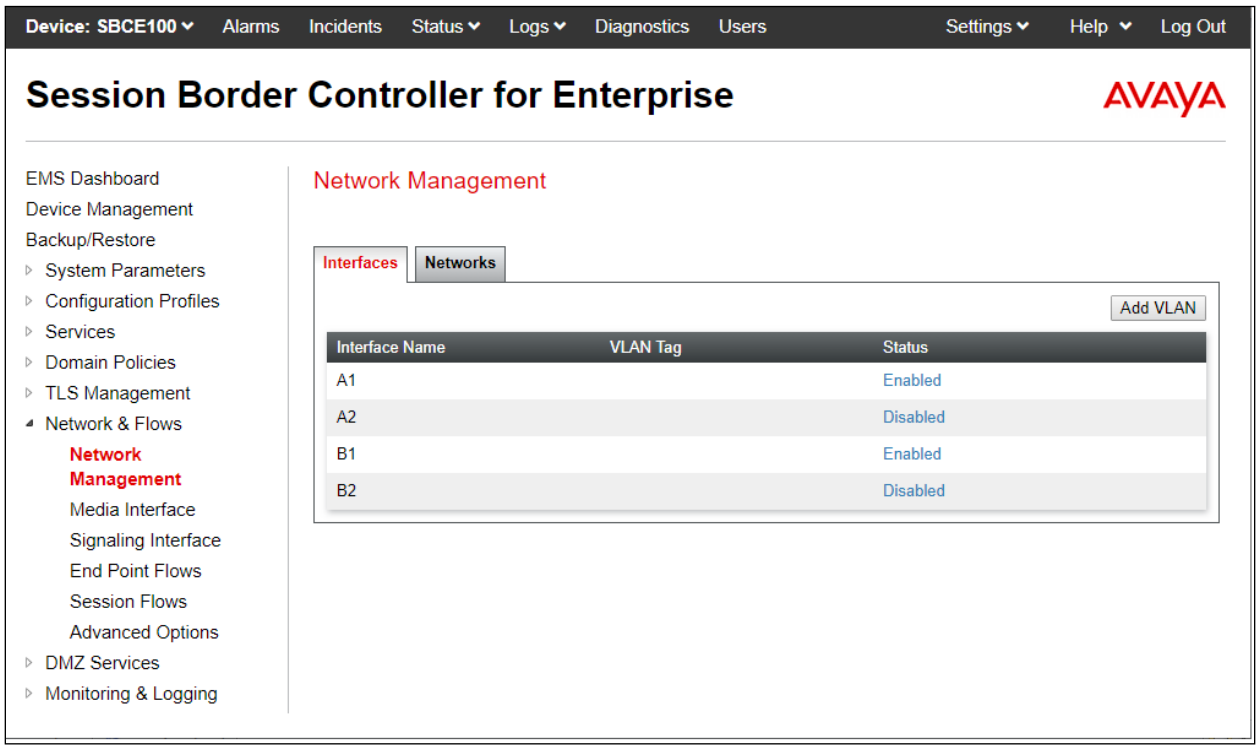
Primary DNS	10.33.100.60
Secondary DNS	8.8.8.8
DNS Location	DMZ
DNS Client IP	10.33.1.51

Management IP(s)

IP #1 (IPv4)	10.33.10.100

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

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



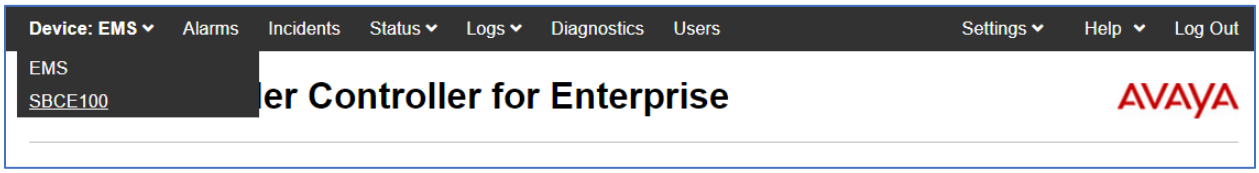
7.3. TLS Management

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

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

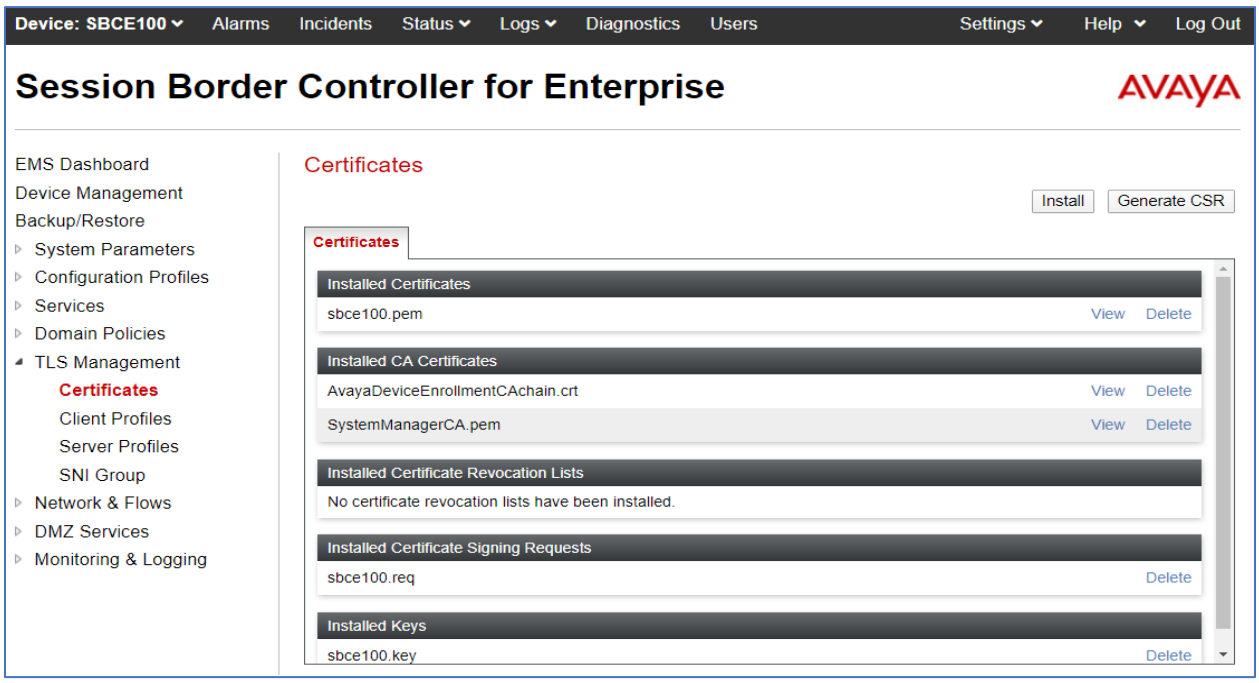
7.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

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



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

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

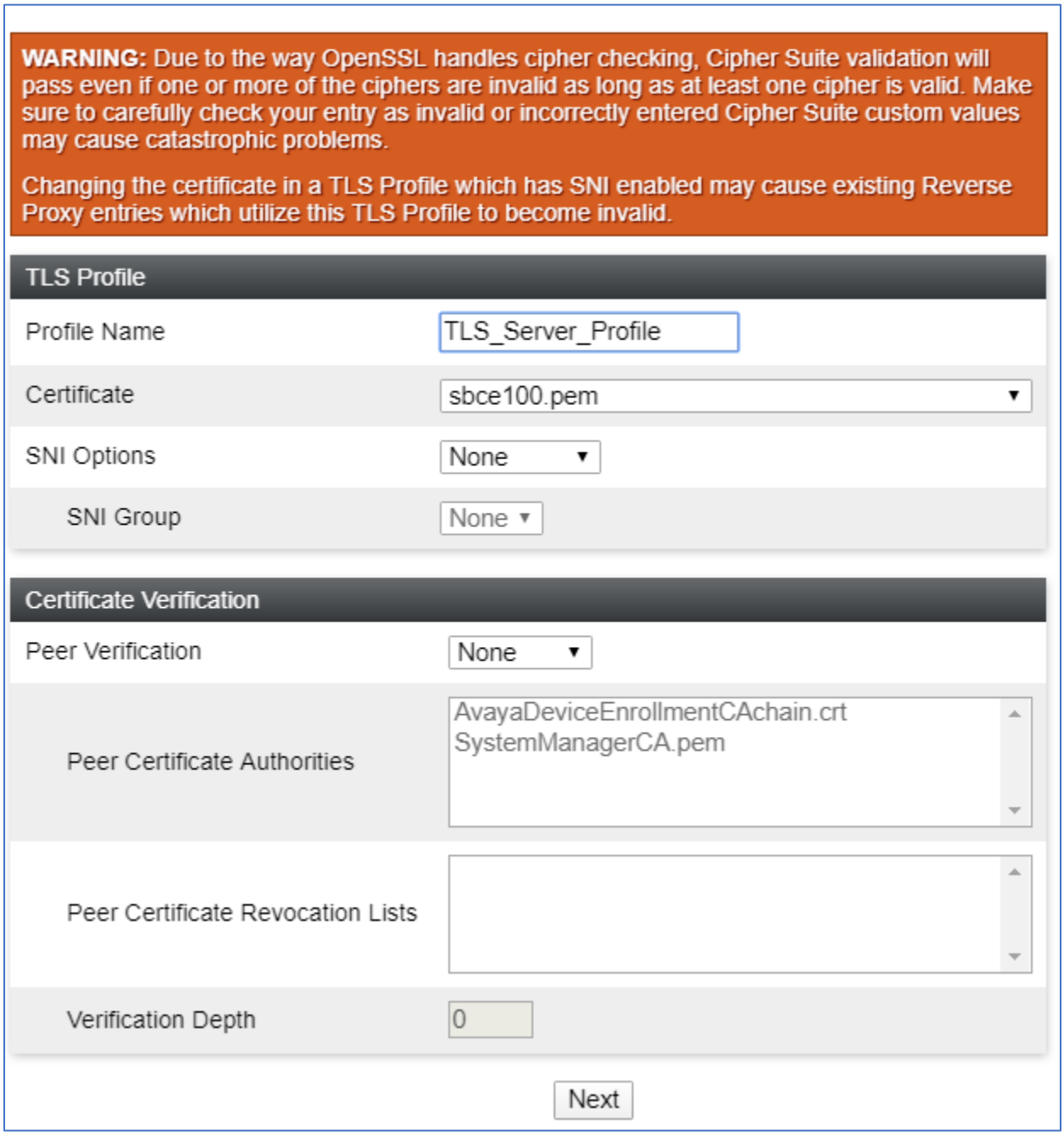


7.3.2. Server Profiles

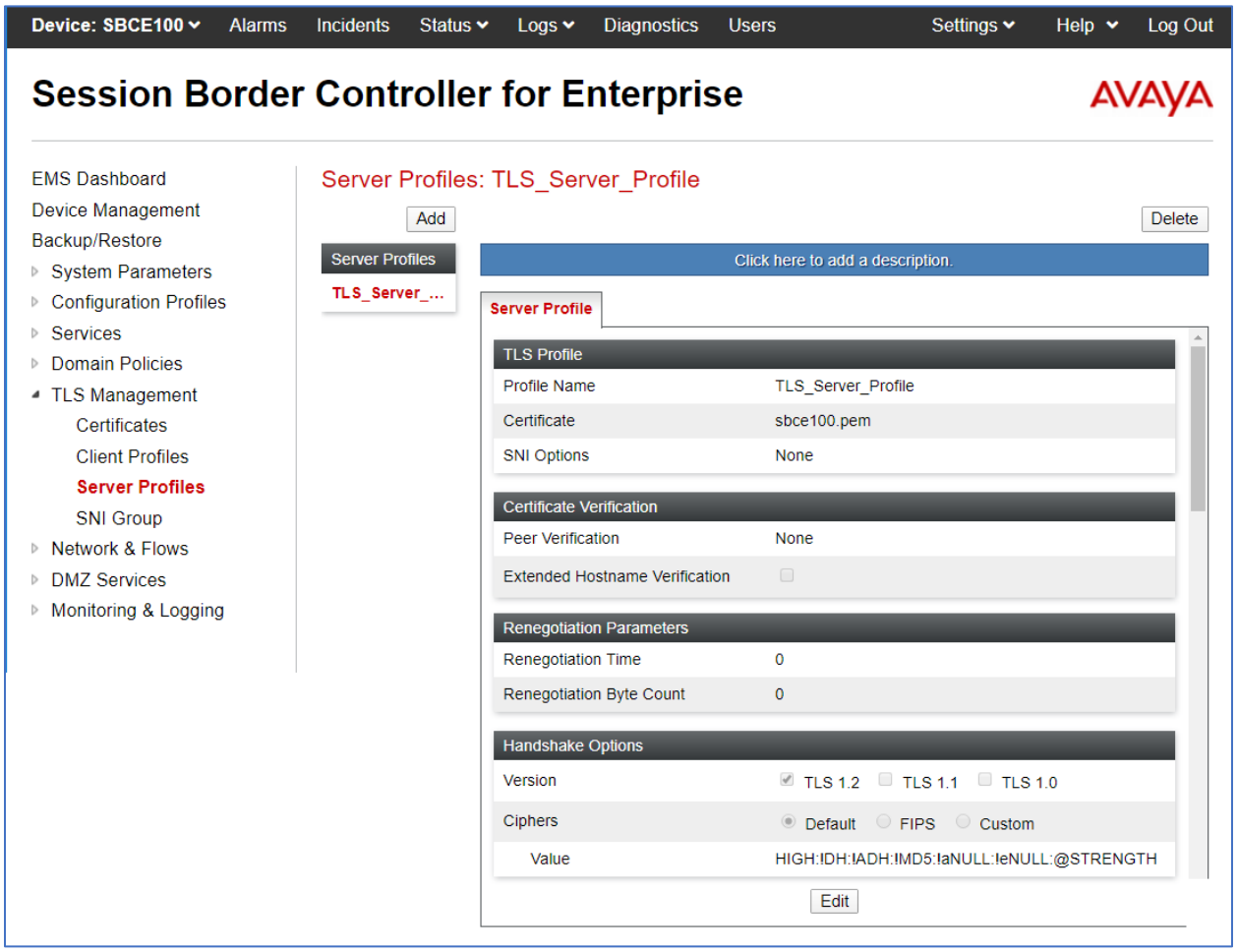
Step 1 - Select **TLS Management → Server Profiles** and click on **Add**. Enter the following:

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

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



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

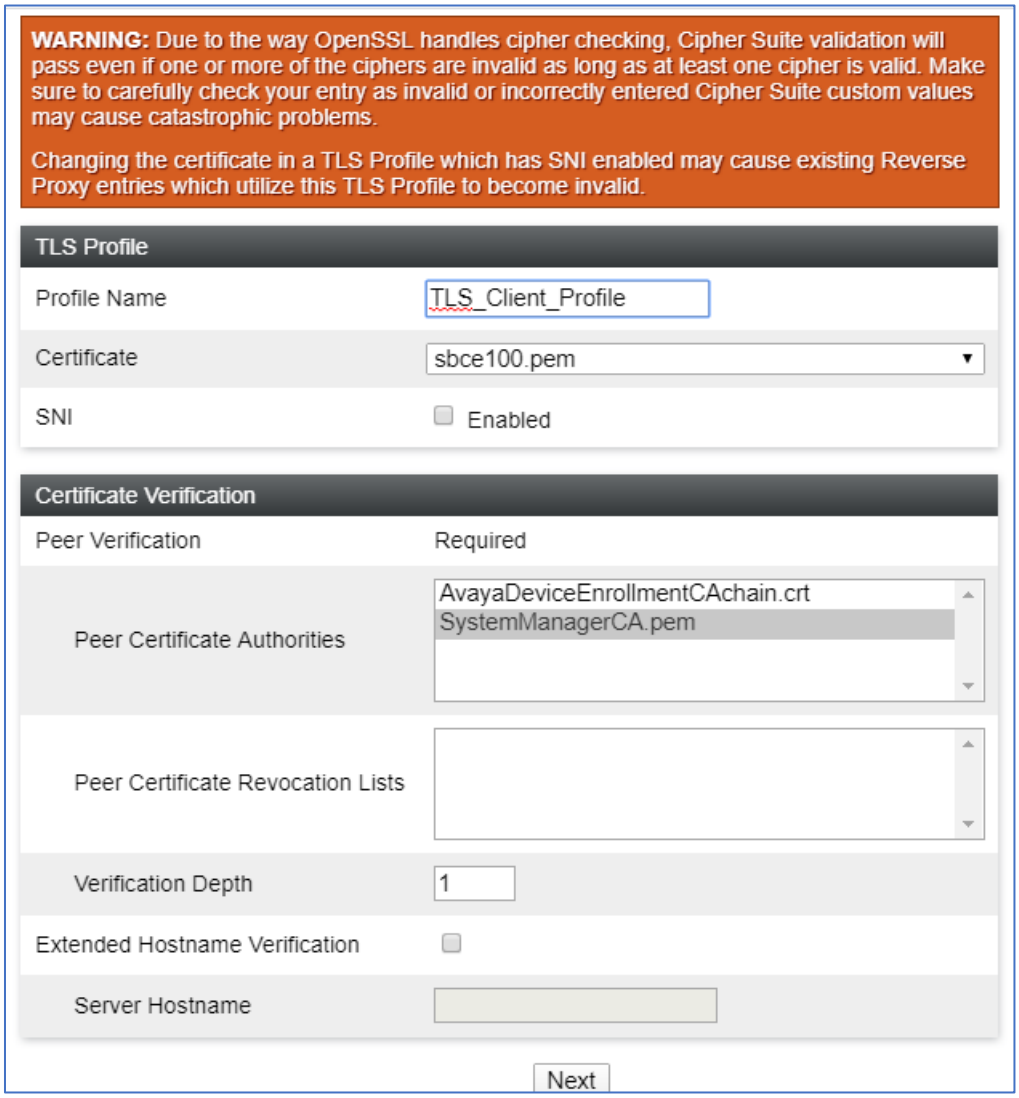


7.3.3. Client Profiles

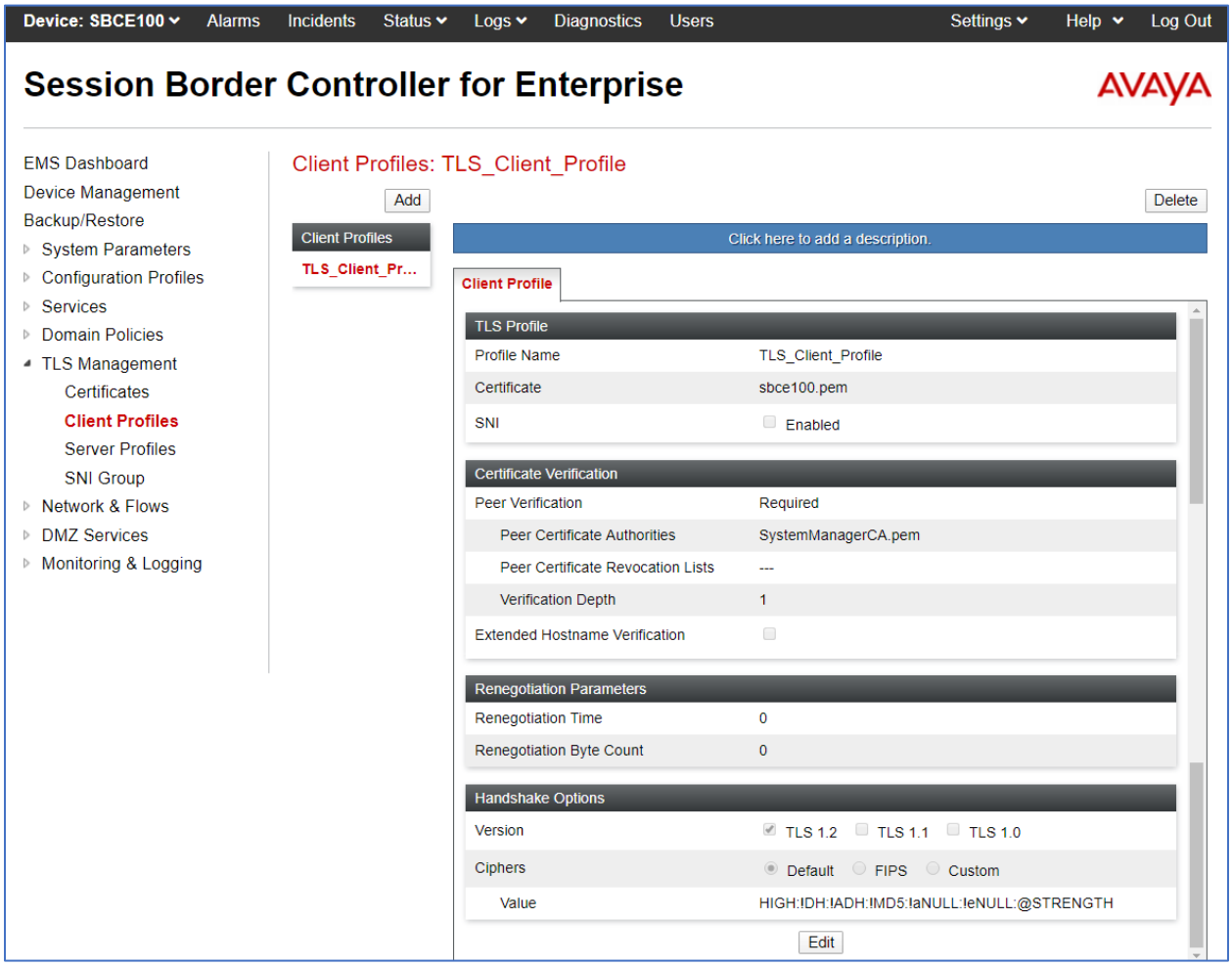
Step 1 - Select **TLS Management → Server Profiles**, and click on **Add**. Enter the following:

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

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



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

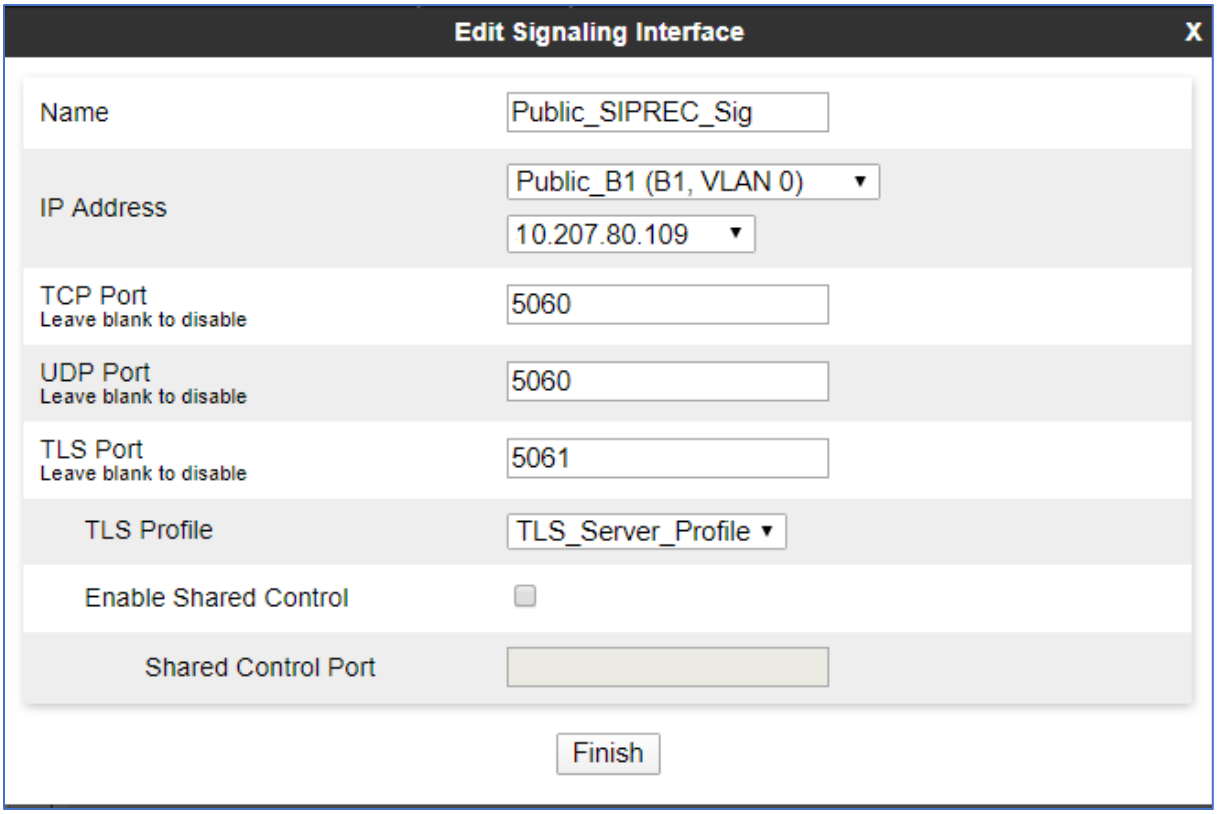


7.4. Signaling Interface

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

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

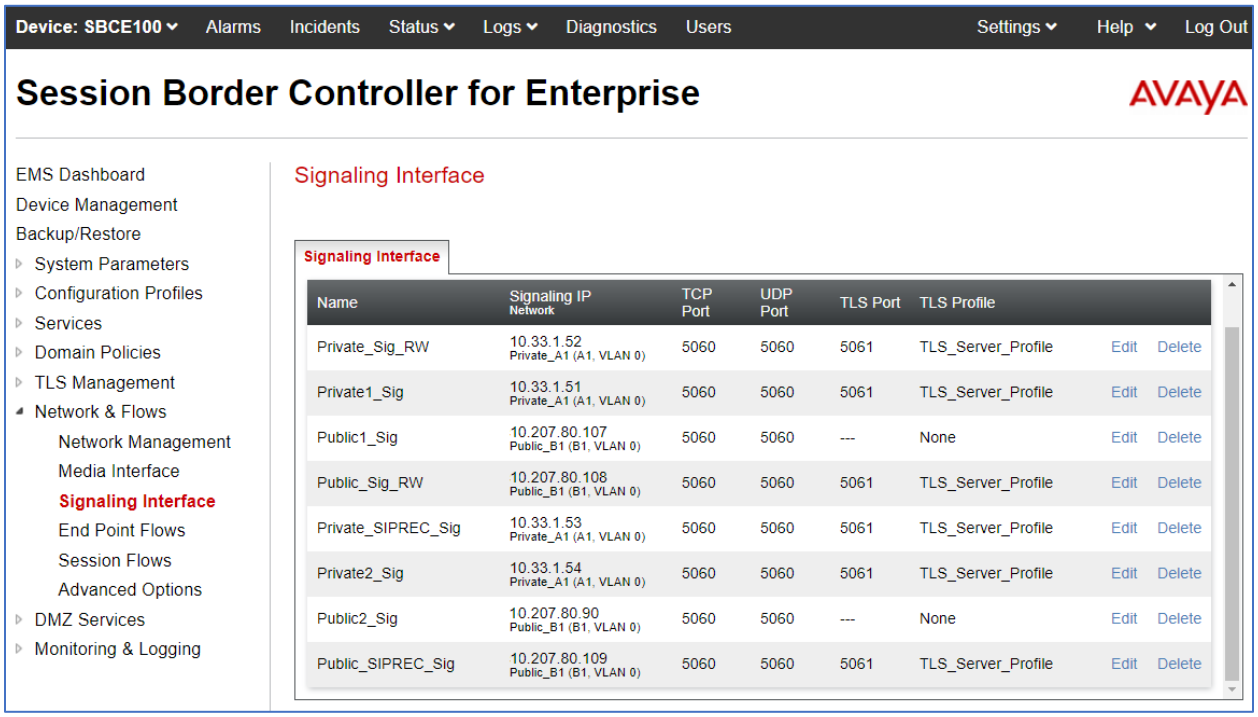
- **Name**: enter a descriptive name.
- For the internal interface, set the **IP Address** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **IP Address** to the IP address associated with the public interface (B1) defined in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



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

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

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



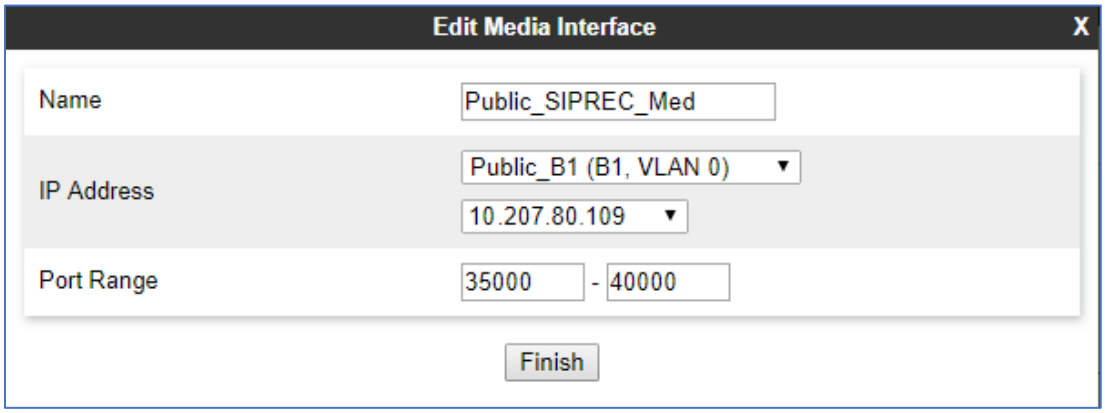
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
Private_Sig_RW	10.33.1.52 Private_A1 (A1, VLAN 0)	5060	5060	5061	TLS_Server_Profile	Edit	Delete
Private1_Sig	10.33.1.51 Private_A1 (A1, VLAN 0)	5060	5060	5061	TLS_Server_Profile	Edit	Delete
Public1_Sig	10.207.80.107 Public_B1 (B1, VLAN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

7.5. Media Interface

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

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

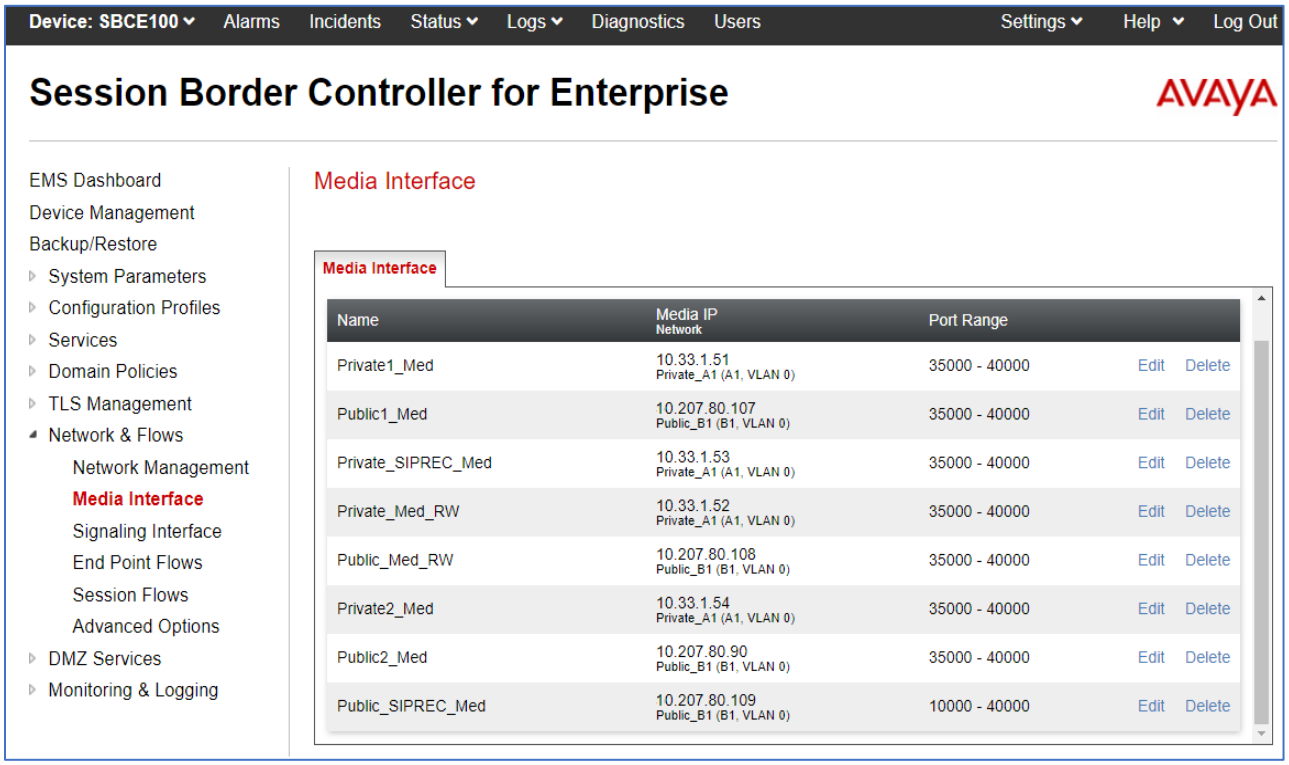
- **Name**: enter a descriptive name.
- For the internal media interface, set the **IP Address** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set the **IP Address** to the IP address associated with the public interface (B1) defined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



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

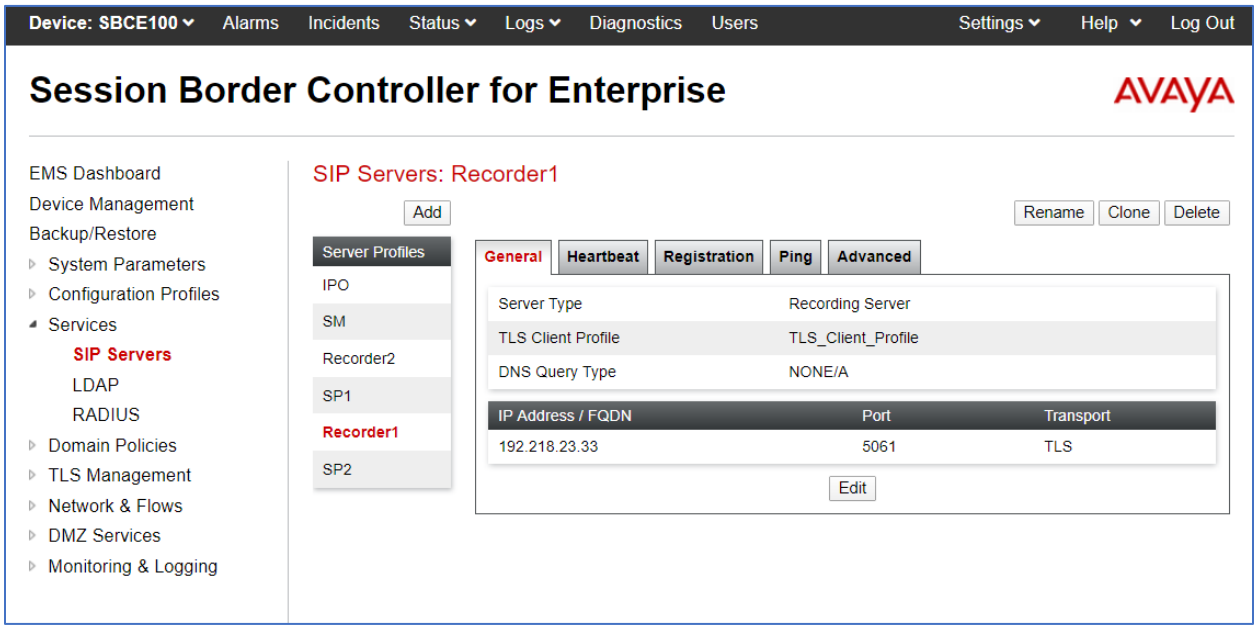
Name	IP address	Description
Private1_Med	10.33.1.51	The private media interface connects to enterprise endpoints such as media gateway and agent endpoints
Public1_Med	10.207.80.107	The public media interface connects to media gateway of Service Provider
Private_Med_RW	10.33.1.52	The private media interface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

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



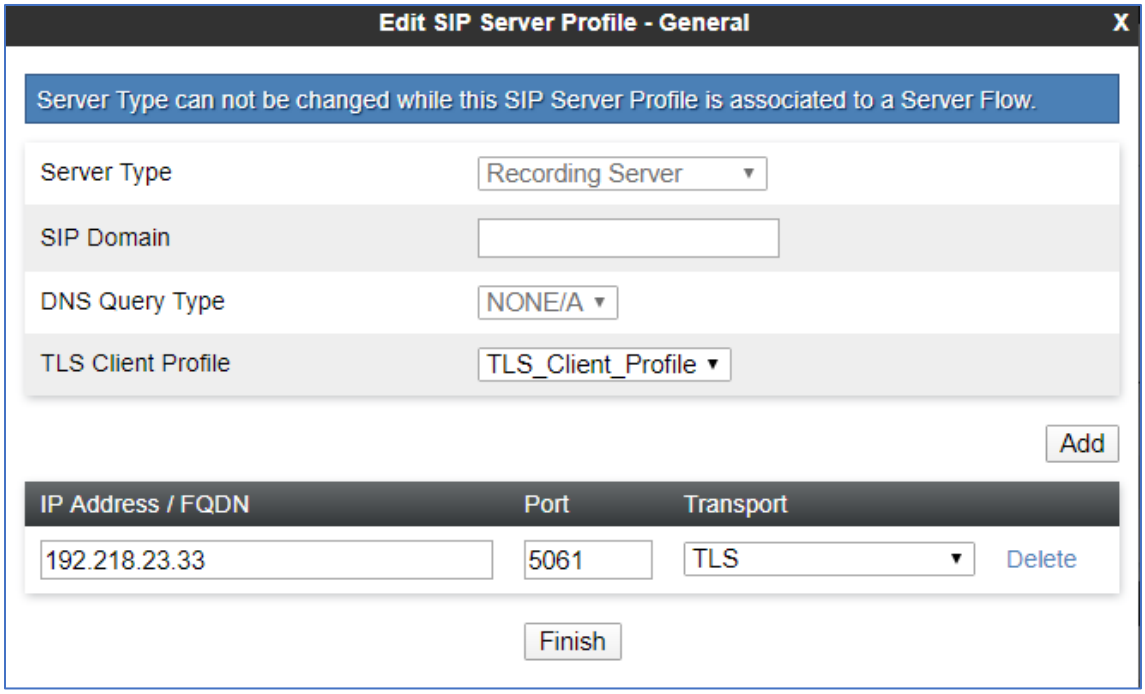
7.6. Server Configuration

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



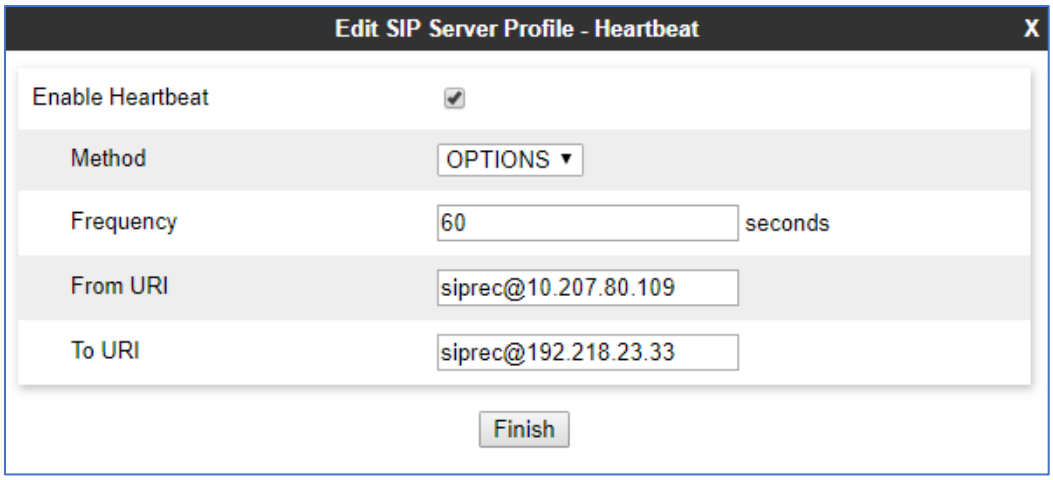
For the compliance test, there were two SIP server profiles: **Recorder1** and **Recorder2** created for the Cogito recording servers. The screenshot shows the **Edit SIP Server Profile - General** tab parameters as follow.

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

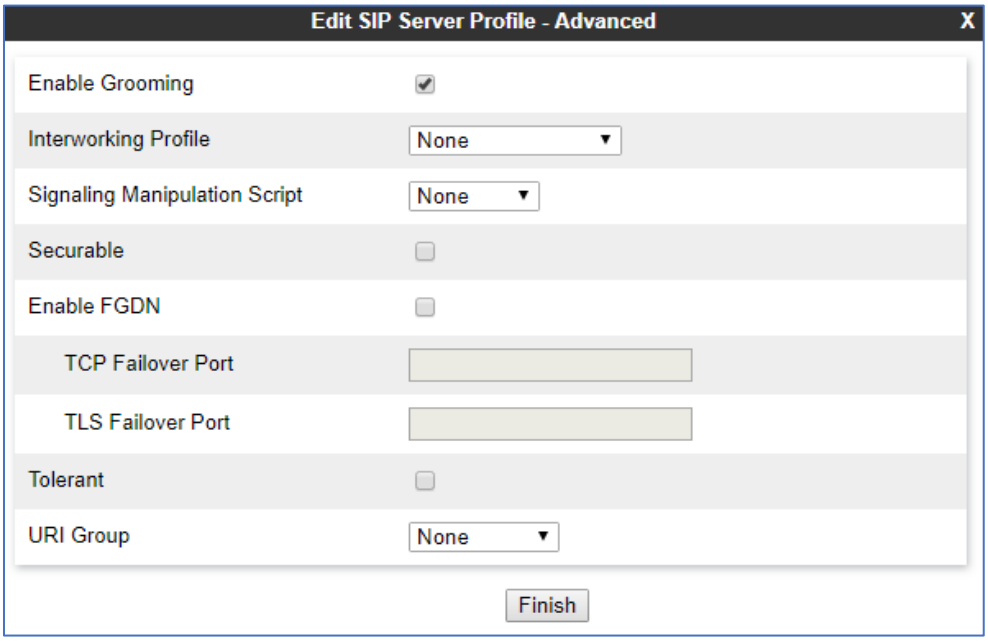


In the **Heartbeat** tab, enter following parameters as shown in the screenshot below.

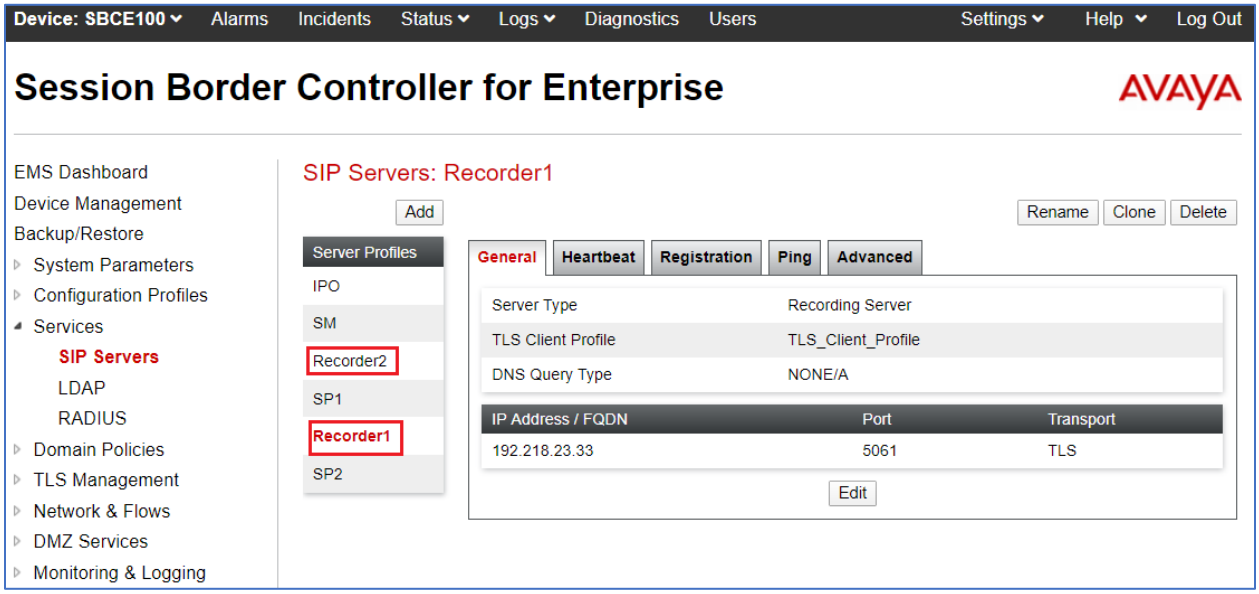
- **Enable Heartbeat**: checked.
- **Method**: select **OPTIONS** in the dropdown menu.
- **Frequency**: enter an interval for the Avaya SBCE sending out OPTIONS to the Cogito recording server.
- **From URI**: enter the uri format as user@domain or user@ipaddress. In the testing, the public IP for SIPREC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



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



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



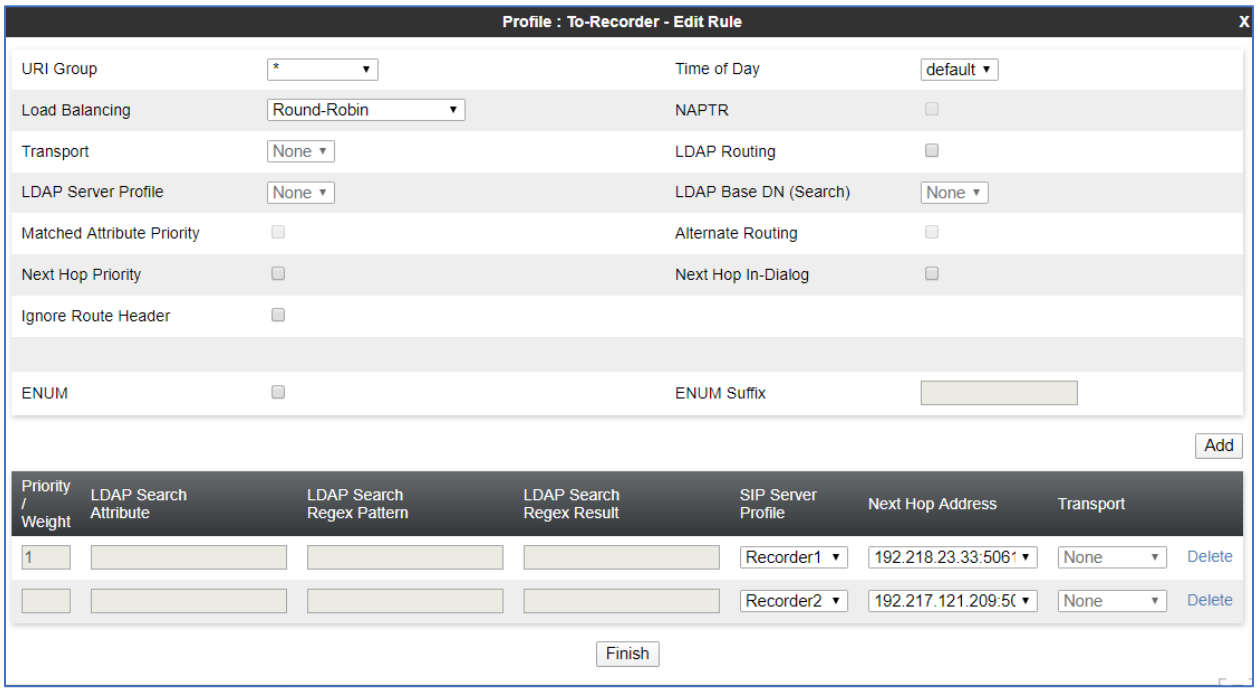
7.7. Routing Configuration

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

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

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

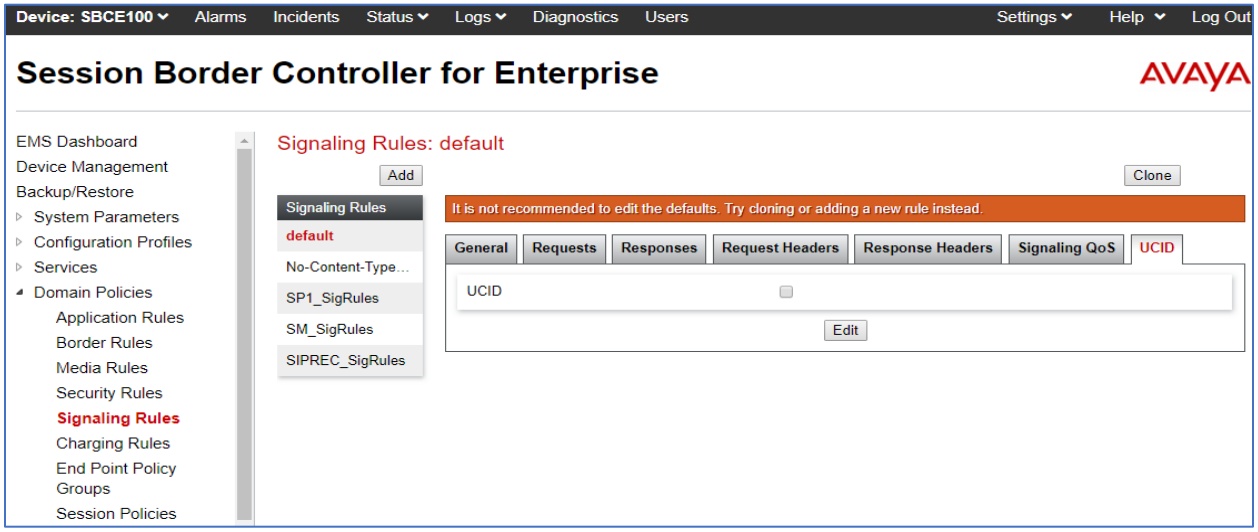
Click **Finish**.



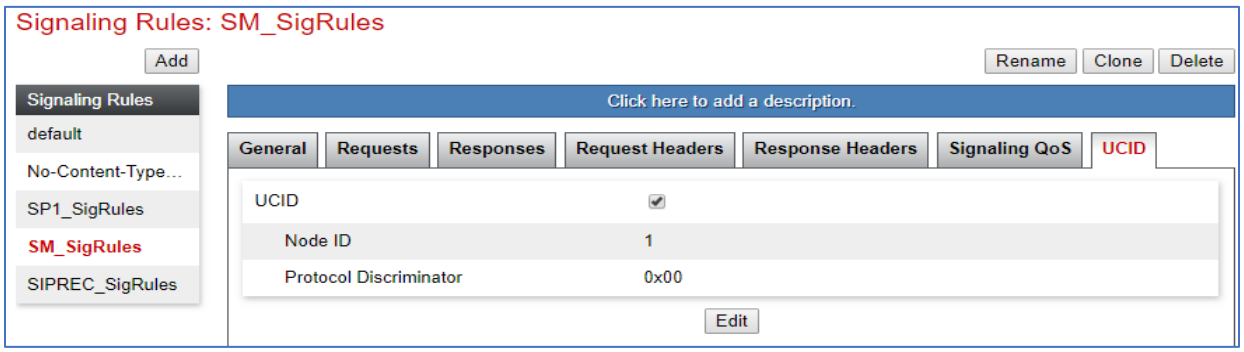
7.8. Signaling Rules

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

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



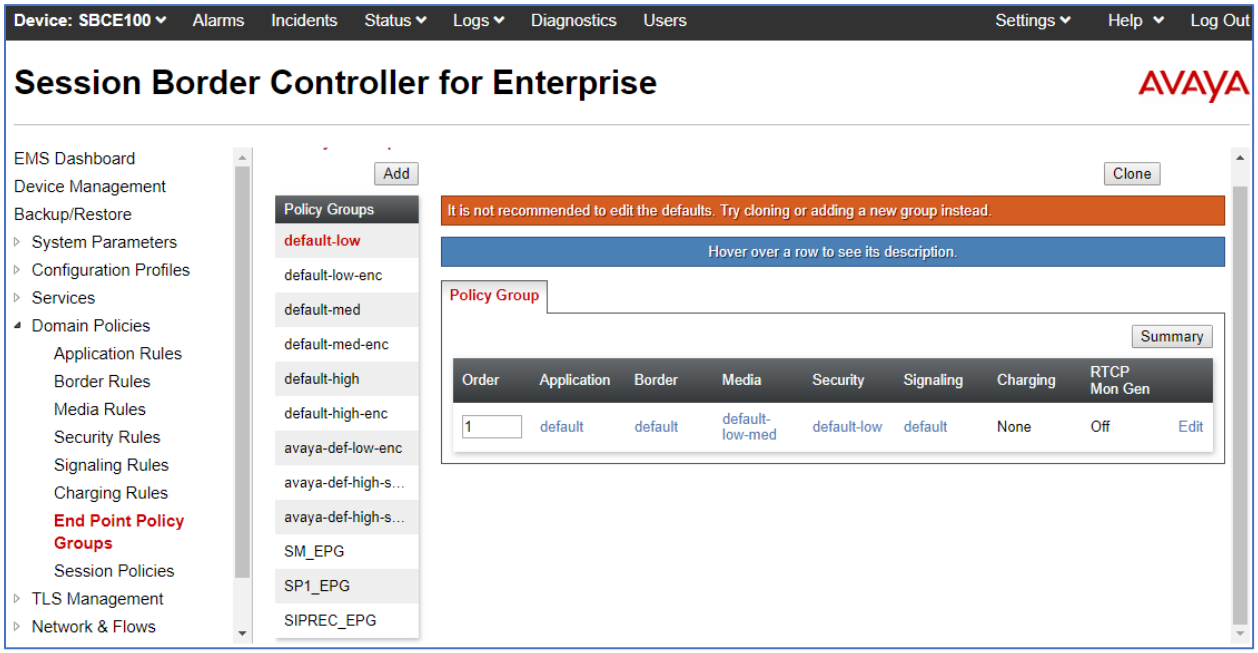
In the testing, there are 3 signaling rules created: **SM_SigRules** and **SP1_SigRules** are previously created for the SIP trunk, and **SIPREC_SigRules** is created for the Cogito recording server. The Signaling rule for Session Manager must have UCID enabled and set the ID number as the same number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



7.9. End Point policy Groups

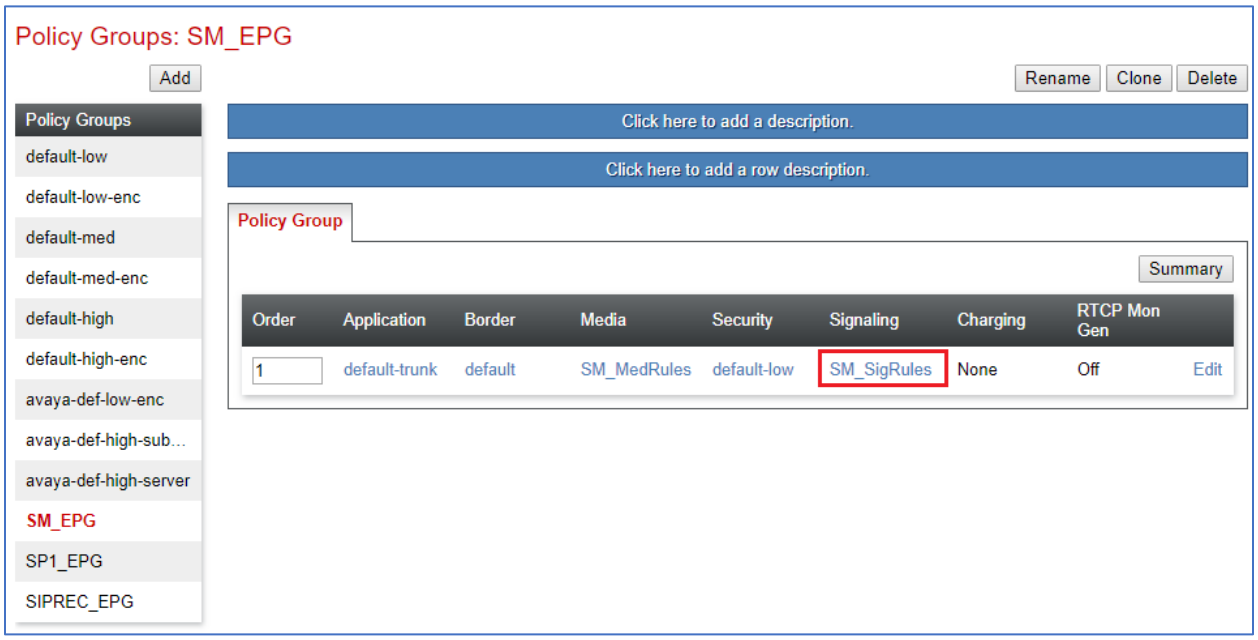
An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and an endpoint (connected server). Thus, an endpoint policy group must be created for Session Manager, Service Provider and the Cogito recording server.

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

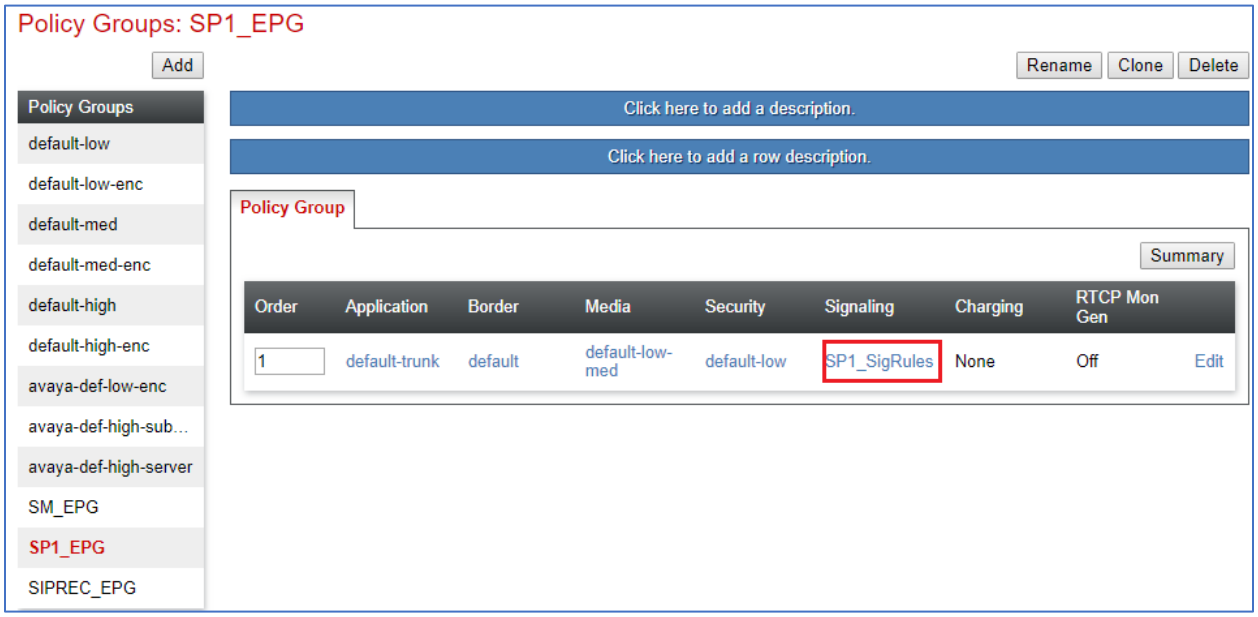


In the testing, there are 3 end point policy groups created: **SM_EPG** and **SP1_EPG** are previously created for the SIP trunk, and **SIPREC_EPG** is created for the Cogito recording server.

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



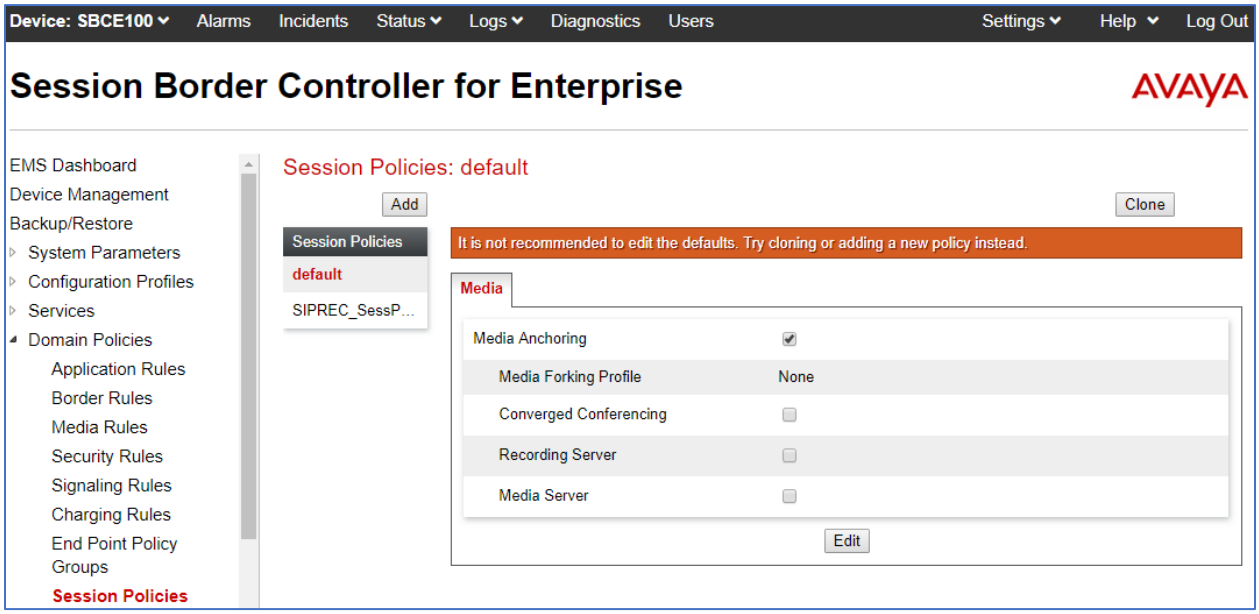
The screenshot below shows the end point policy groups used for Service Provider, **SP1_EPG**. The policy group uses the **SP1_SigRules** created in **Section 7.8** above.



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

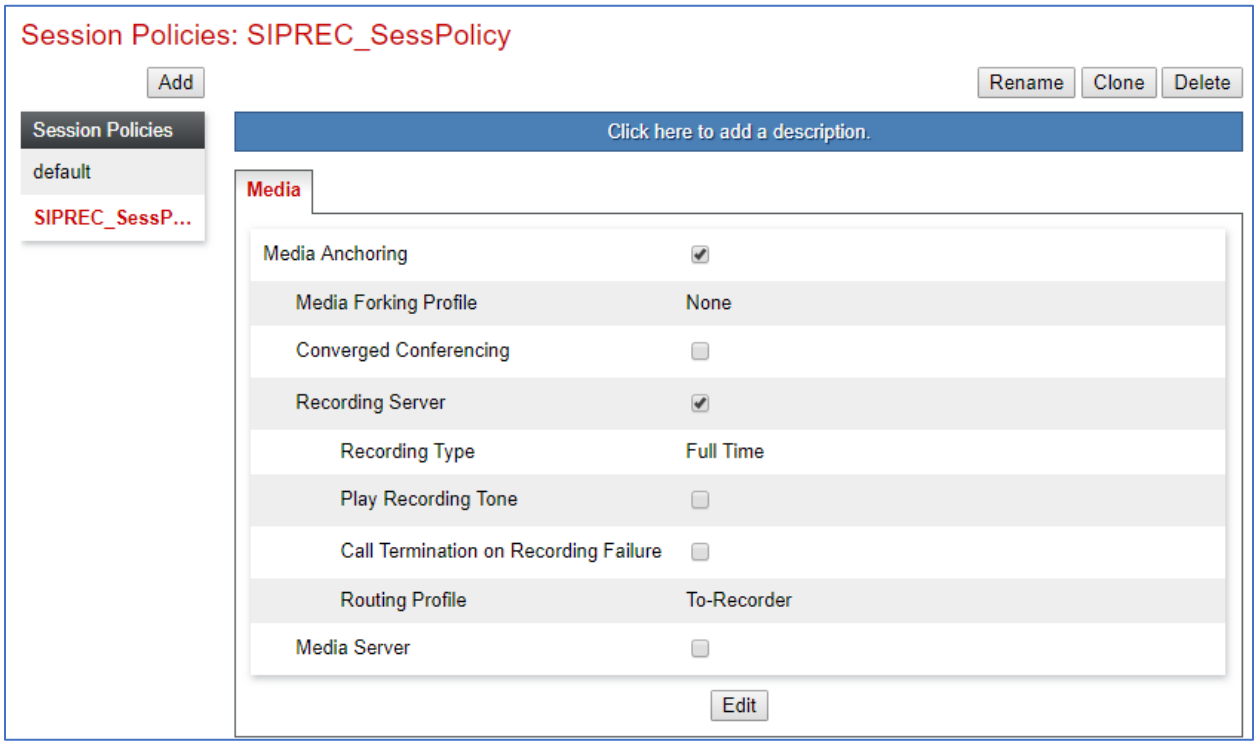
7.10. Session Policies

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.



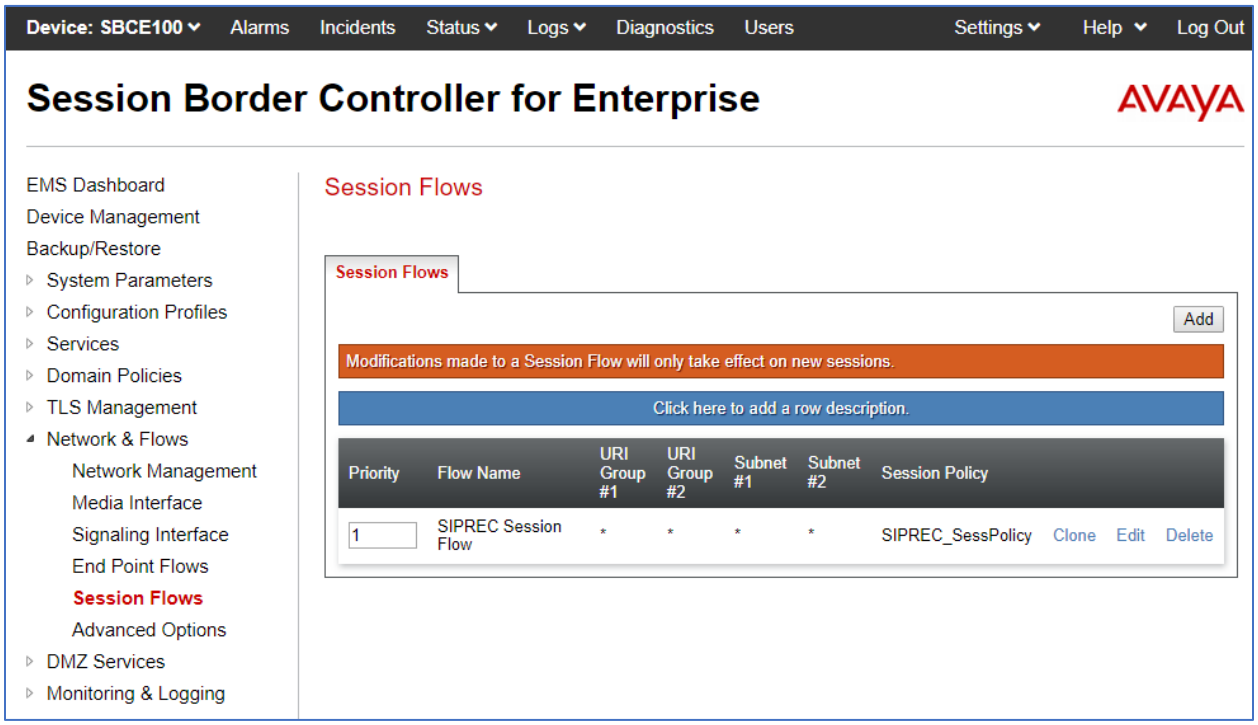
In the testing, the session policy **SIPREC_SessPolicy** is created with configuration as shown below.

- **Media Anchoring**: checked.
- **Recording Server**: checked.
- **Recoding Type**: select **Full Time** in the dropdown menu.
- **Routing Profile**: select the routing profile ***To-Recorder*** as configured in **Section7.7**.



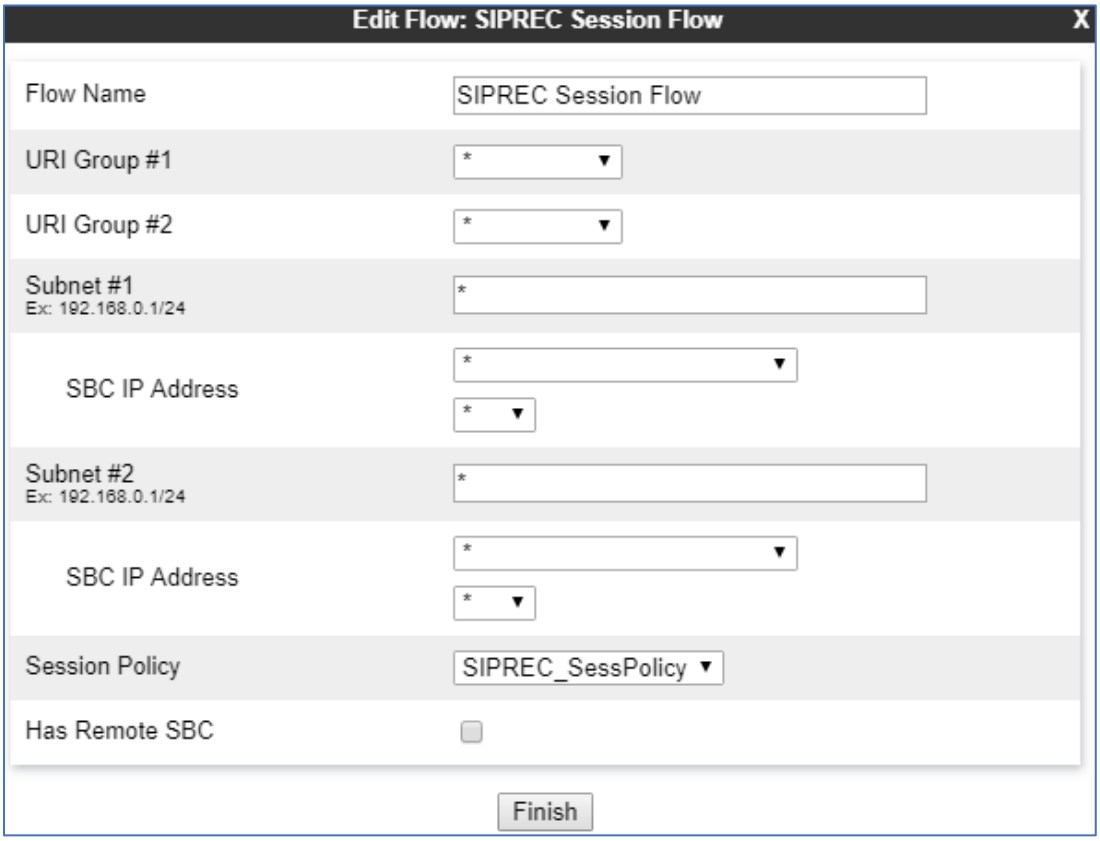
7.11. Session Flows

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



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

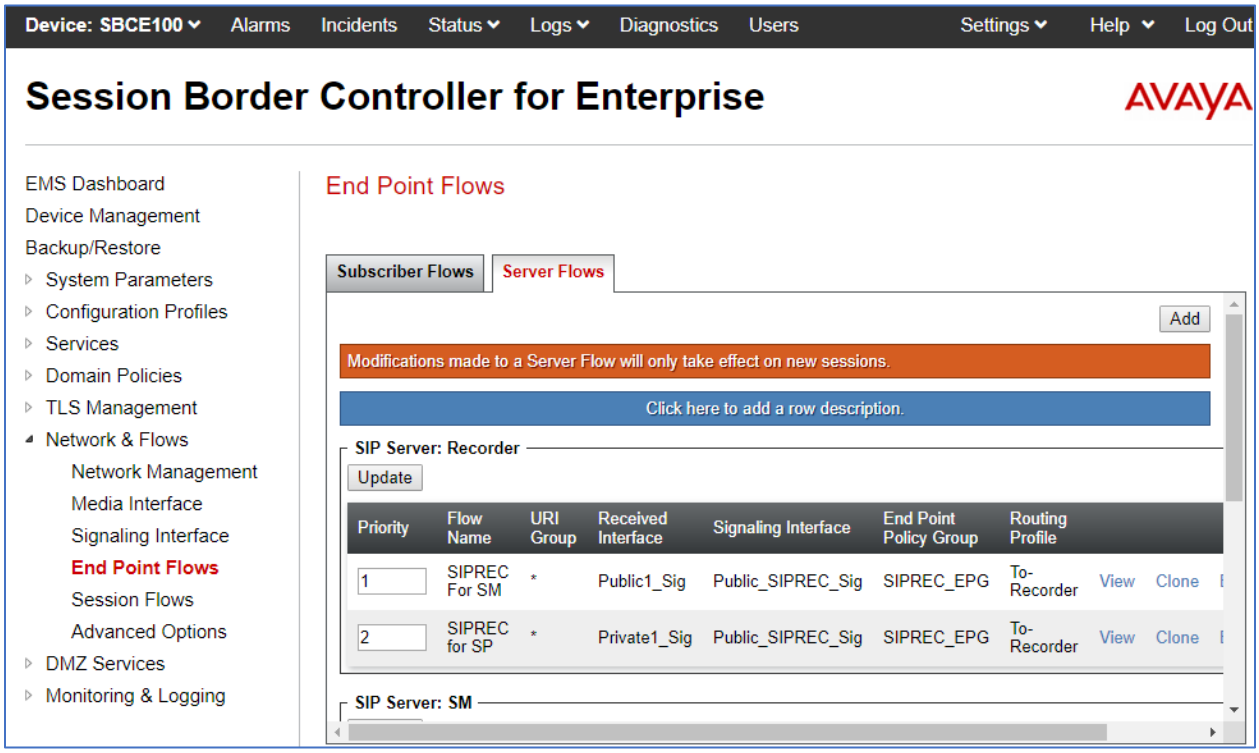
- **Flow Name**: enter a descriptive name.
- **Session Policy**: select the session policy ***SIPREC_SessPolicy*** in the dropdown menu as configured in **Section 7.10**.
- Keep other fields at default values.



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.

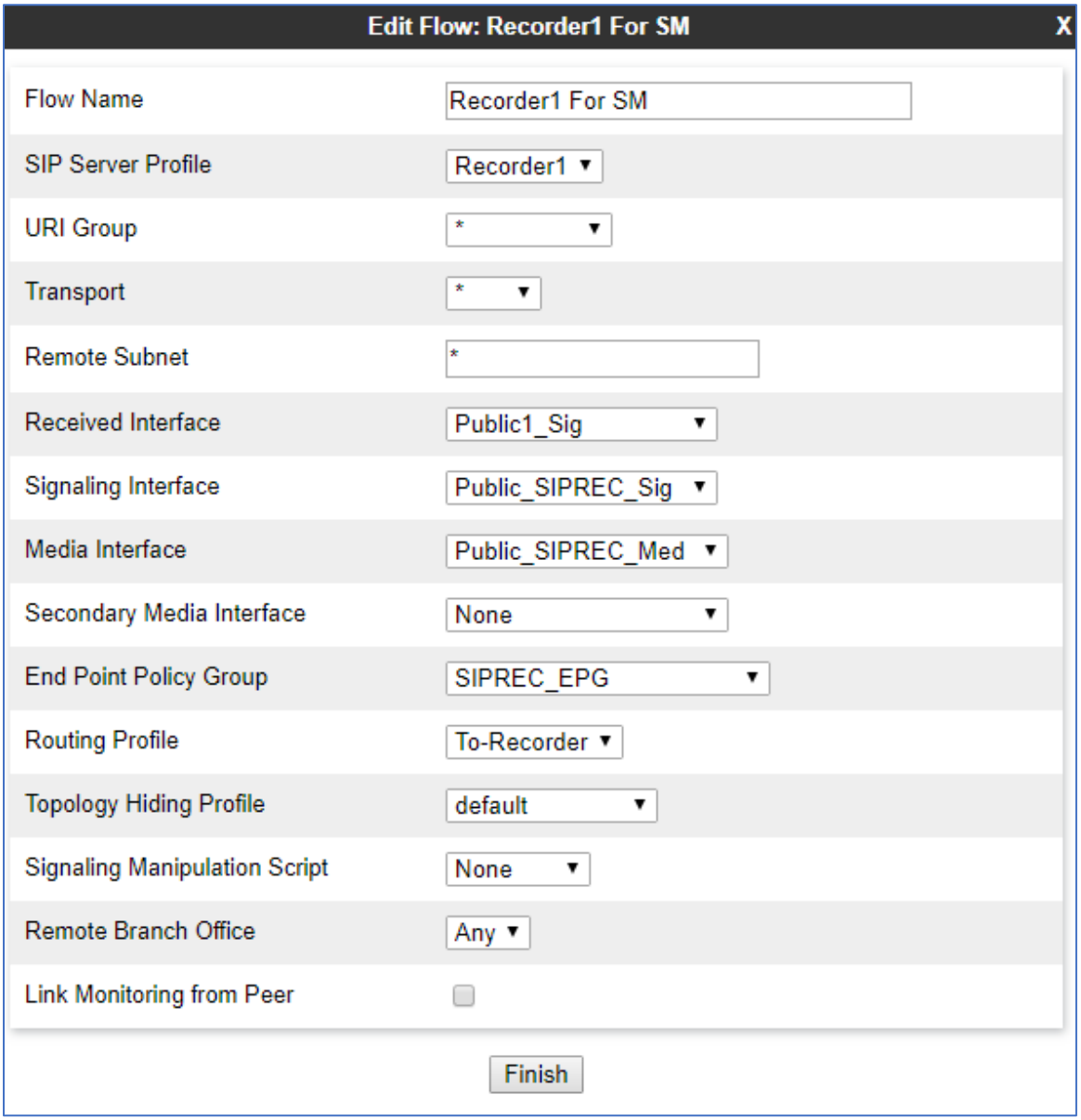


In the testing, there were totally four server flows created for two Cogito recording servers to record both ways from the PSTN to the enterprise (agent device) and from the enterprise (agent device) to the PSTN via the SIP trunk.

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

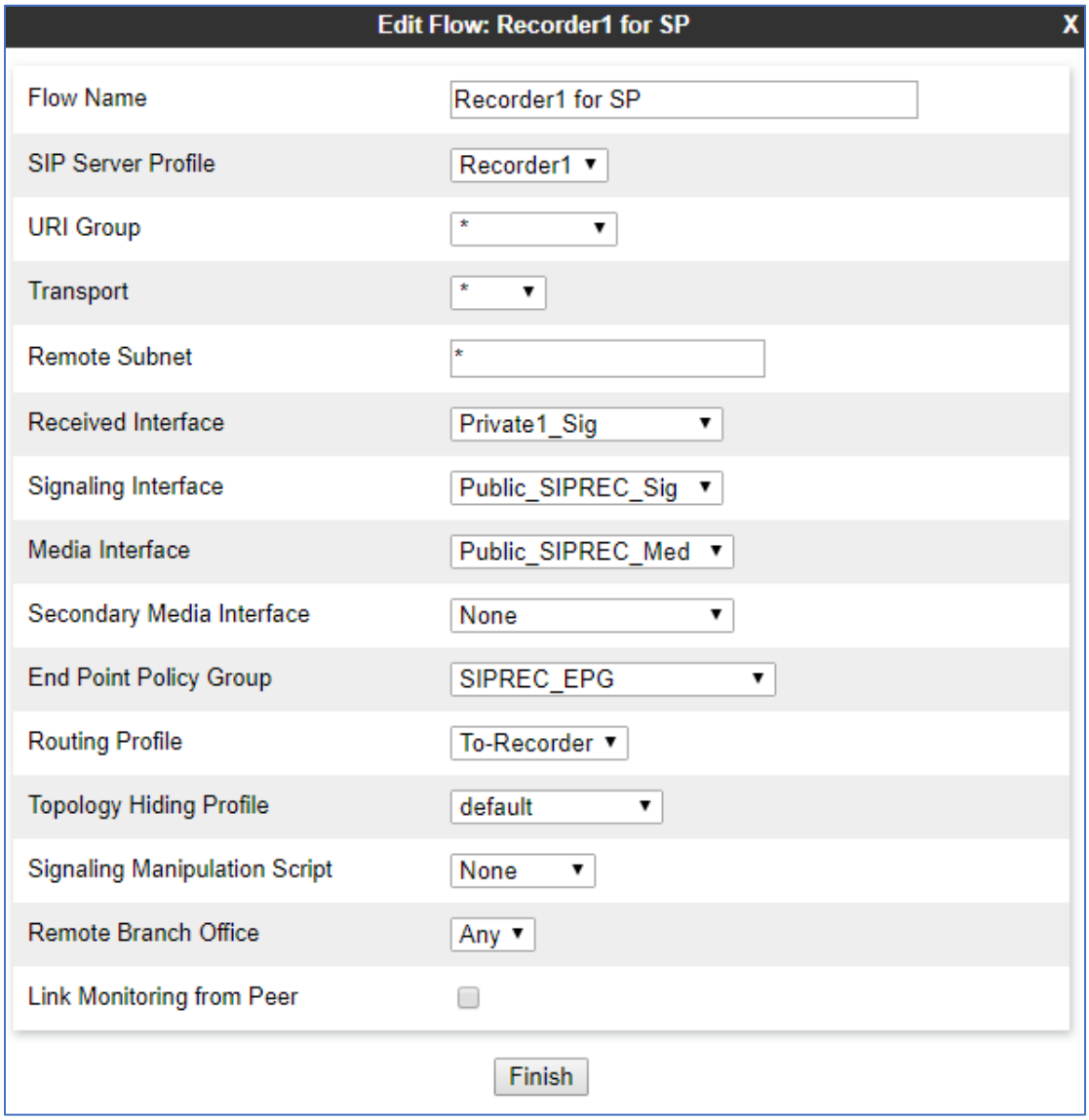
- **Flow Name**: enter a descriptive name, e.g. **Recorder1 For SM**.
- **SIP Server Profile**: select ***Recorder1*** as configured in **Section 7.6**.
- **Received Interface**: select ***Public1_Sig*** in the list. This is the interface receiving the signaling for the server flow from Session Manager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

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



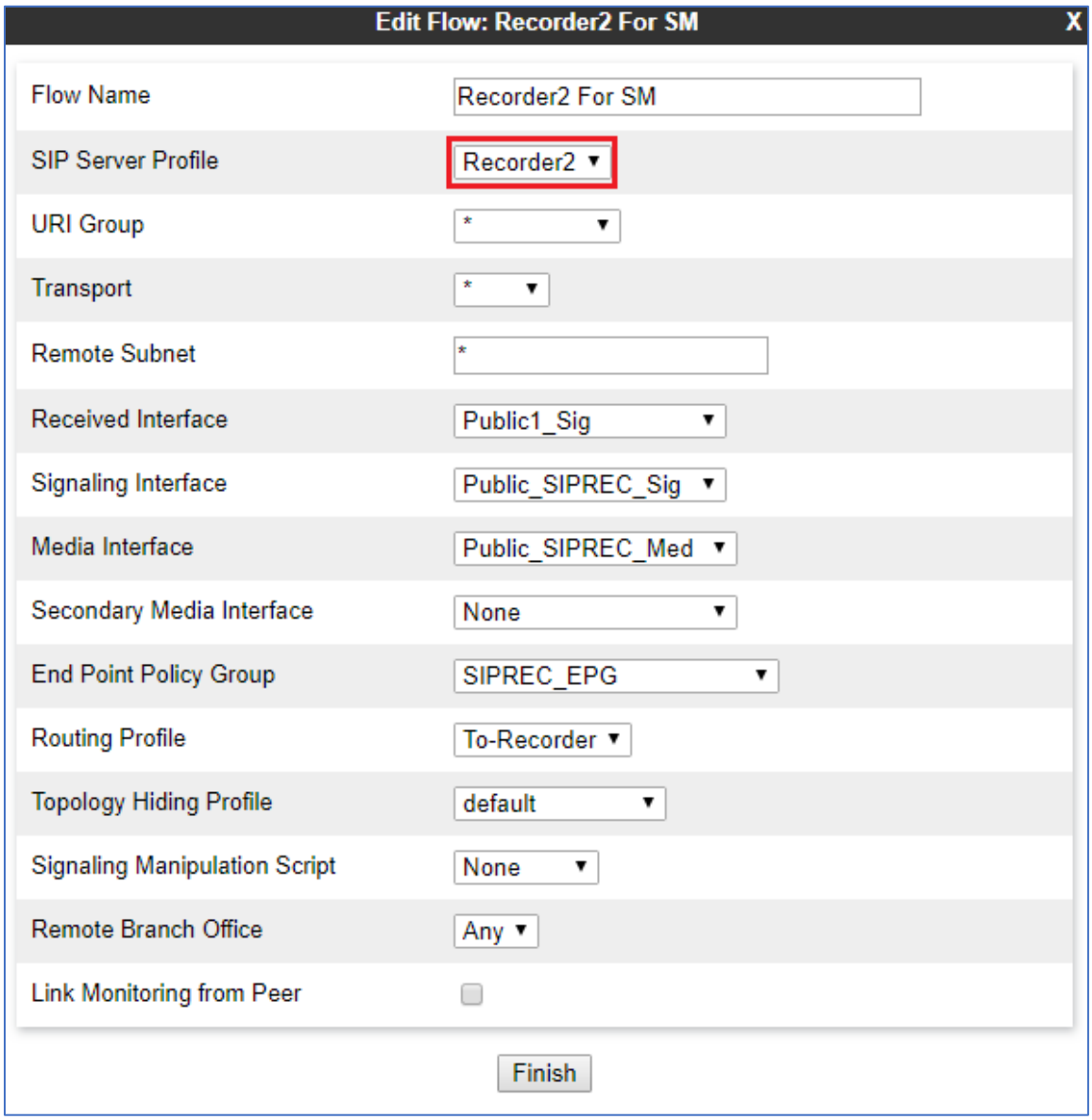
The screenshot below shows the configuration for the Cogito Recorder1 server flow from the Service Provider toward Session Manager, ***Recorder1 For SP***:

- **Flow Name**: enter a descriptive name, e.g. **Redorder1 For SP**.
- **SIP Server Profile**: select ***Recorder*** as configured in **Section 7.6**.
- **Received Interface**: select ***Privarte1_Sig*** in the list. This is the interface receiving the signaling for the server flow from the service provider toward to Session Manager.
- **Signaling Interface**: select ***Public_SIPREC_Sig*** as configured in **Section 7.4**.
- **Media Interface**: select ***Public_SIPREC_Med*** as configured in **Section 7.5**.
- **End Point Policy Group**: select **SIPREC_EPG** as configured in **Section 7.9**.
- **Routing Profile**: select ***To-Recorder*** as configured in **Section 7.7**.
- Keep other fields at the default values.



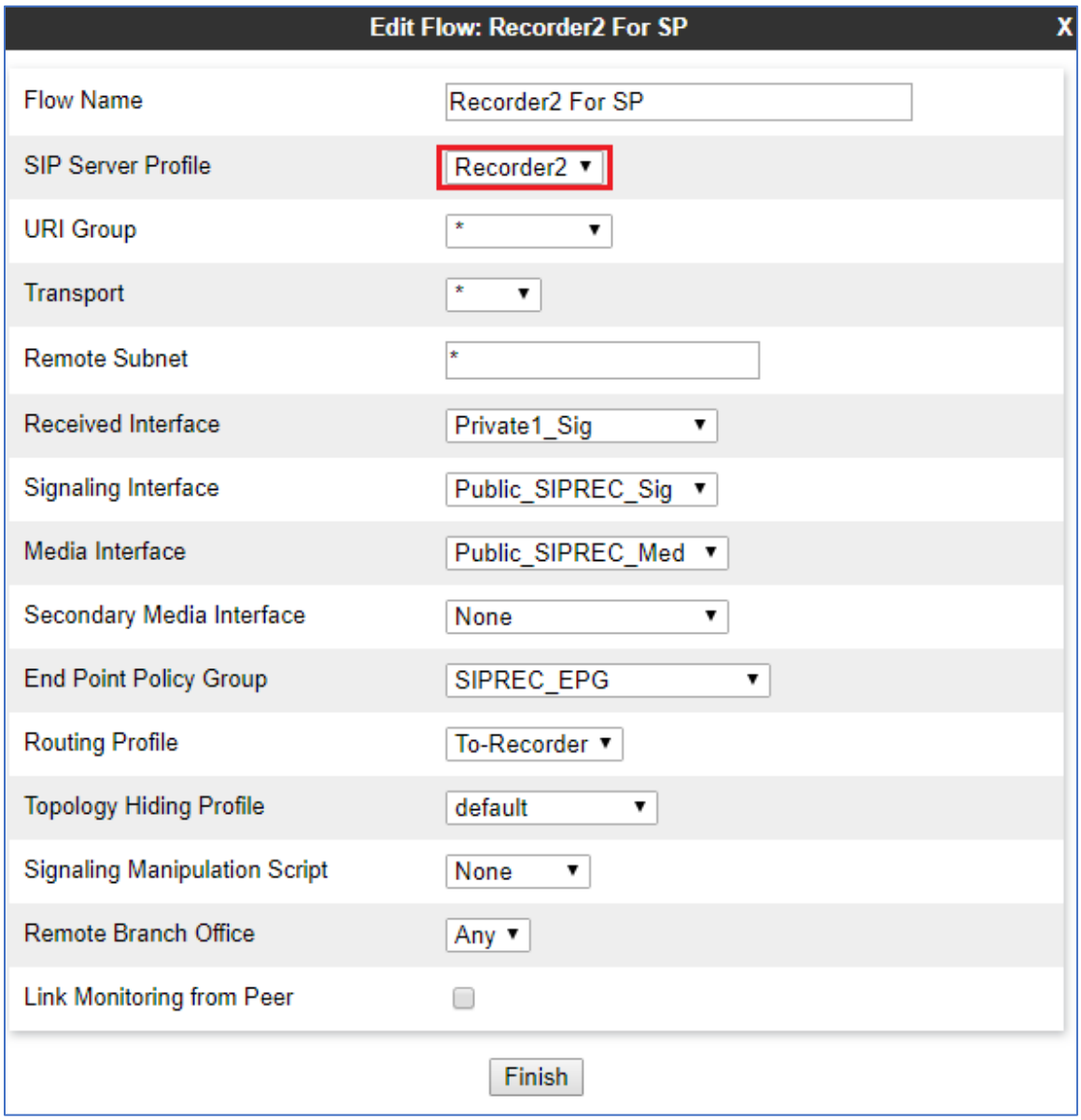
The screenshot below shows the configuration for the Cogito Recorder2 server flow from Session Manager toward the Service Provider, ***Recorder2 For SM***:

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



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

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



8. Configure Cogito Recording

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

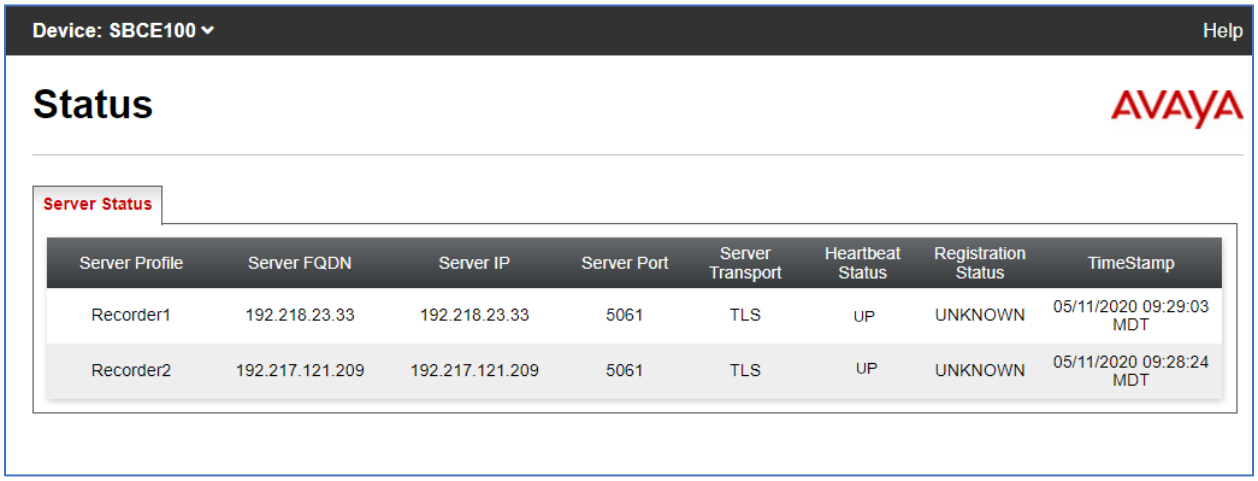
For configuring TLS, the certificate authority (CA) of System Manager is used to create the certificate for the Cogito SIP recording server.

9. Verification Steps

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

9.1. Verify Server Status in SBCE

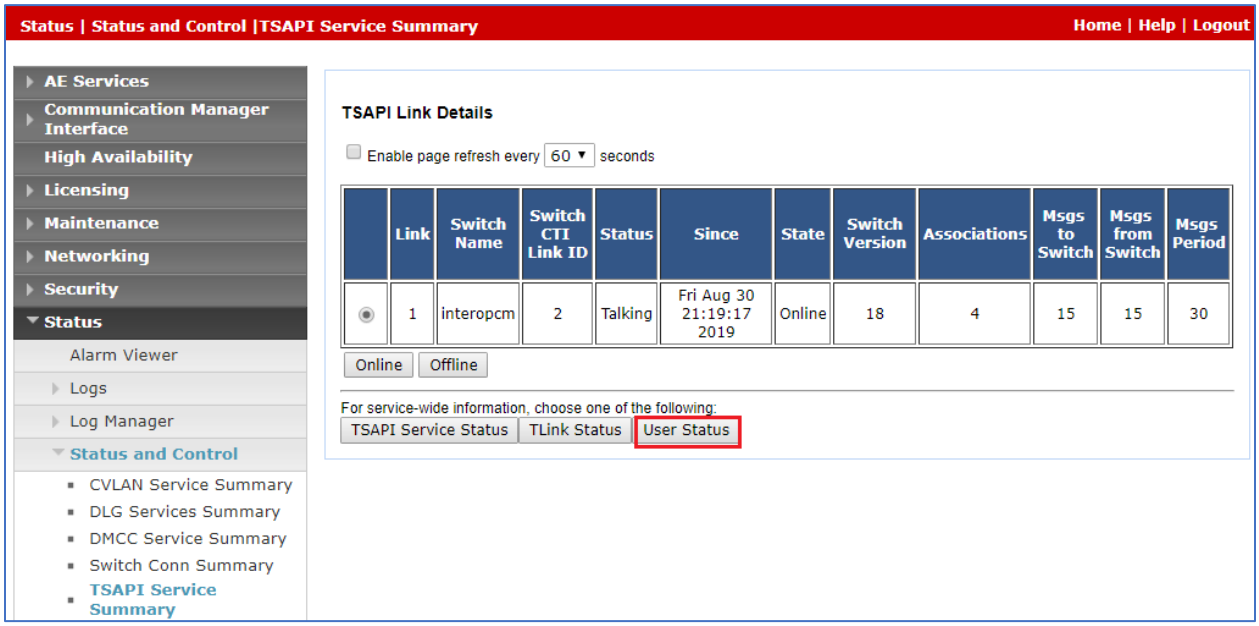
Verify the status of the Cogito recording servers in the Avaya SBCE, from the horizontal menu navigate to **Status → Server Status** (not shown). The status in the **Heartbeat Status** column should display as "**UP**".



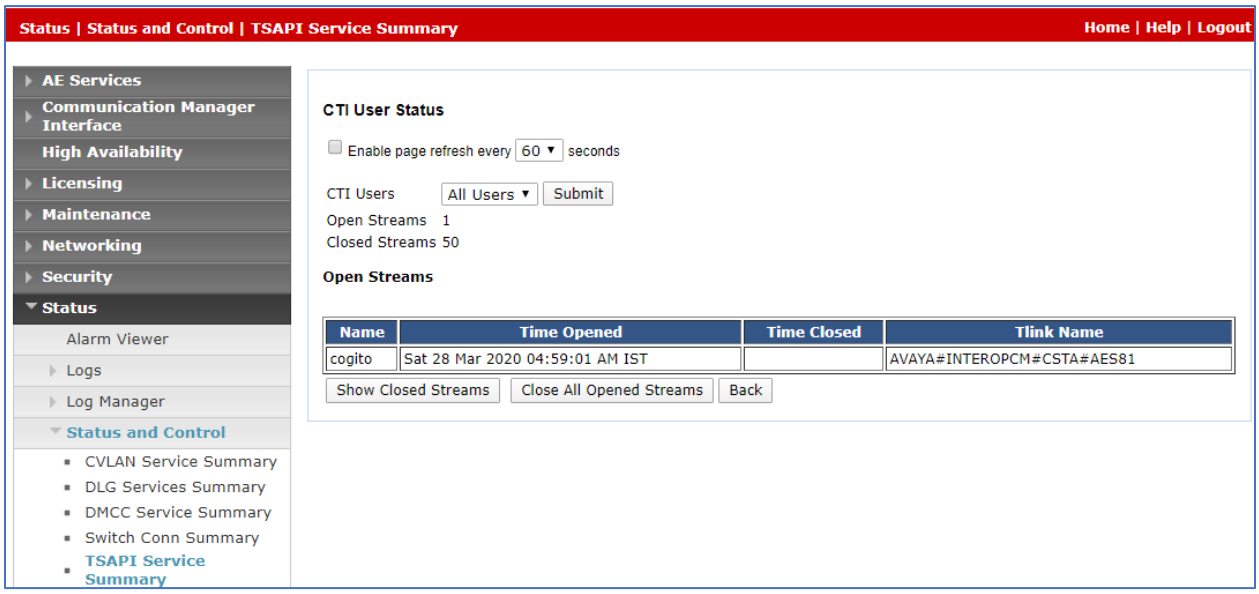
Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
Recorder1	192.218.23.33	192.218.23.33	5061	TLS	UP	UNKNOWN	05/11/2020 09:29:03 MDT
Recorder2	192.217.121.209	192.217.121.209	5061	TLS	UP	UNKNOWN	05/11/2020 09:28:24 MDT

9.2. Verify AES Connection

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



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



9.3. Verify Status of Agent in CM

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

```
list monitored-station

                              MONITORED STATION

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

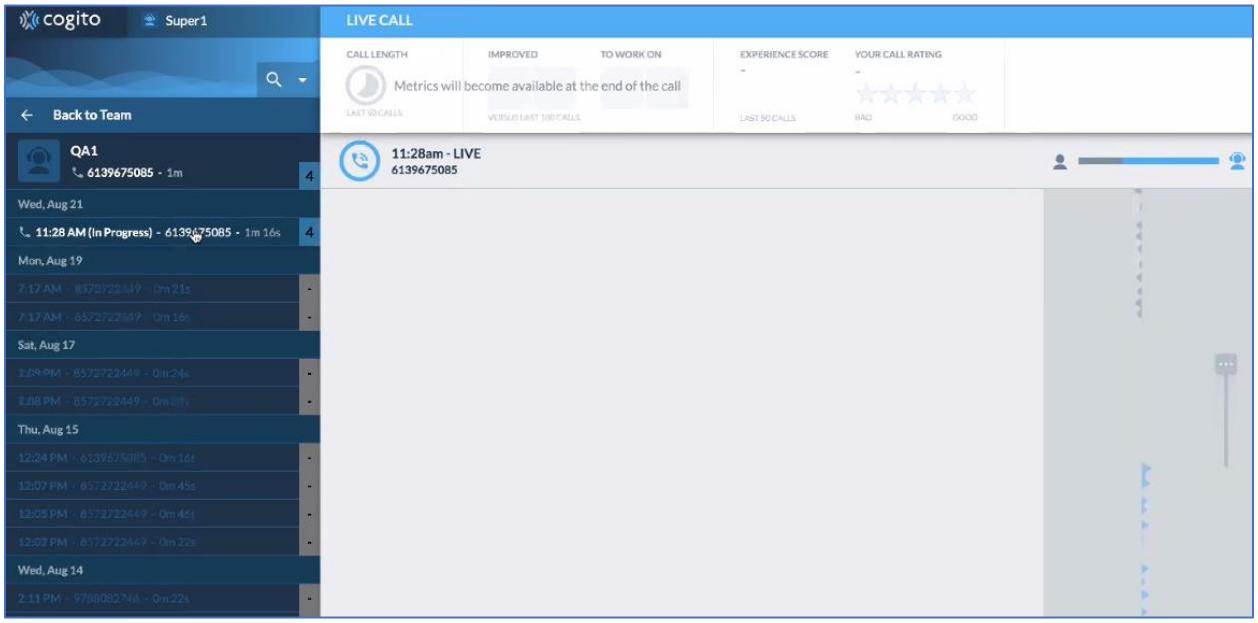
Use the command "**list agent-loginID**" to verify the status of agent. Note that the agents need to be logged in for Cogito recording server to trigger the recording.

```
list agent-loginID
                              AGENT LOGINID
Login ID         Name            Extension      Dir Agt  AAS/AUD    COR AgPr SO
                Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv

1000             Agent 1000      3301                                 1   lvl
                  1/01     /       /       /       /       /       /       /
1001             Agent 1001      3401                                 1   lvl
                  1/01     /       /       /       /       /       /       /
1002             Agent 1002      3403                                 1   lvl
```

9.4. Verification Steps for SIPREC:

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



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

10. Conclusion

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

11. Additional References

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

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

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.