Avaya Solution & Interoperability Test Lab

Application Notes for ASAPP Voice Desk 2.2 with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® Application Enablement Services 8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for ASAPP Voice Desk 2.2 with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® Application Enablement Services 8.1.

ASAPP Voice Desk is an audio transcription solution that uses the Java Telephony Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations, and the SIP-based Media Recording interface from Avaya Session Border Controller for Enterprise to capture media for calls between agents and the PSTN. The captured media are transcribed in real time by ASAPP Voice Desk and displayed on the agent desktop.

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 ASAPP Voice Desk 2.2 (ASAPP) with Avaya Session Border Controller for Enterprise (SBCE) 8.1 and Avaya Aura® Application Enablement Services 8.1.

ASAPP is an audio transcription solution that uses the Java Telephony Application Programming Interface (JTAPI) from Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and the SIP-based Media Recording (SIPREC) interface from SBCE to capture media for calls between agents and the PSTN. The captured media are transcribed in real time and displayed on the agent desktop connected to ASAPP Voice Desk via an Internet browser.

The ASAPP solution is a cloud offering that consists of multiple servers hosted by Amazon Web Services (AWS). In the compliance testing, the ASAPP solution resided on AWS and connected to the Avaya products via a VPN connection. The CTI Adapter server component of the ASAPP solution is responsible for JTAPI connection with Application Enablement Services and contains the Avaya JTAPI Windows Client. The Media Gateway Proxies server component of the solution is responsible for SIPREC connection with SBCE.

When there is an active inbound ACD call at the monitored agent station, ASAPP is informed of the call via JTAPI events and starts the transcription with captured media from the SIPREC interface. The JTAPI events are also used to determine when to stop the transcription.

JTAPI is a client-side interface to the Telephony Services Application Programming Interface (TSAPI) on Application Enablement Services. As such, these Application Notes will describe the required configurations for creation and connectivity to the TSAPI service.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the ASAPP application, the application automatically established JTAPI connection with Application Enablement Services and requested device monitoring.

For the manual part of testing, each call was handled manually at the agent.

The serviceability test cases were performed manually by disconnecting/reconnecting the VPN connection to ASAPP.

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 these Application Notes, the interfaces between ASAPP and Avaya products included encrypted JTAPI and non-encrypted SIPREC, as requested by ASAPP.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on ASAPP:

- Use of JTAPI/TSAPI in areas of event notification and value queries.
- Use of SIPREC to capture media from SBCE.
- Proper transcription for call scenarios involving agent drop, customer drop, hold, resume, simultaneous calls, long duration, multiple agents, transfer, and conference.

The serviceability testing focused on verifying the ability of ASAPP to recover from adverse conditions, such as disconnecting and reconnecting the VPN connection to ASAPP.

2.2. Test Results

All test cases were executed and verified. The following were observations on ASAPP from the compliance testing.

- The current ASAPP release only transcribes inbound ACD calls and only supports H.323 agents. In addition, agents are required to use the Avaya Agent for Desktop softphone application. The Avaya Agent for Desktop softphone application in H.323 mode was used in the compliance testing.

- Two-way conversation as part of an internal call is not transcribed by nature of SIPREC integration.

- Three-way conversation as part of conference scenarios is not transcribed by ASAPP per design.

- In the conference scenarios, after PSTN drops from the call, should the conference-from agent drop next then the transcription can move to the conference-to agent as the last remaining agent on the call.

- By design, SBCE does not support codec negotiation with Call Recording Servers such as ASAPP, however, ASAPP will always select G.711 over G.729 when appears in the codec list and therefore can lead to codec incompatibility and result in no transcription. The workaround is to configure the relevant G.711 variant as the only codec on the codec set used by agent stations as required by ASAPP.

- ASAPP requires all transfer-to and conference-to destinations to be monitored including supervisors.

- As part of ASAPP deployment, the ASAPP Solutions Architects need to observe and configure SDP naming to reflect the order of audio streams from the SBCE in the customer network. In the compliance testing, the party labeling in the initial transcriptions were reversed. After updating the configuration for audio stream order on ASAPP, party labeling in subsequent transcriptions were corrected.

- Disrupted calls such as abandoned calls by PSTN while ringing at agent can stay on the tab of an agent browser and get cleared by the auto-end service after 24 hours. This did not have an adverse impact on transcription for subsequent calls with creation of new tabs.

2.3. Support

Technical support on ASAPP can be obtained through the following:

- **Phone :** +1 (212) 658-0990
- **Email :** info@asapp.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of connectivity between Communication Manager, Application Enablement Services, Session Manager, SBCE, and of call center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, ASAPP monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
Skill Group	61001, 61002
Agent Station	65001, 65002
Agent ID	65881, 65882

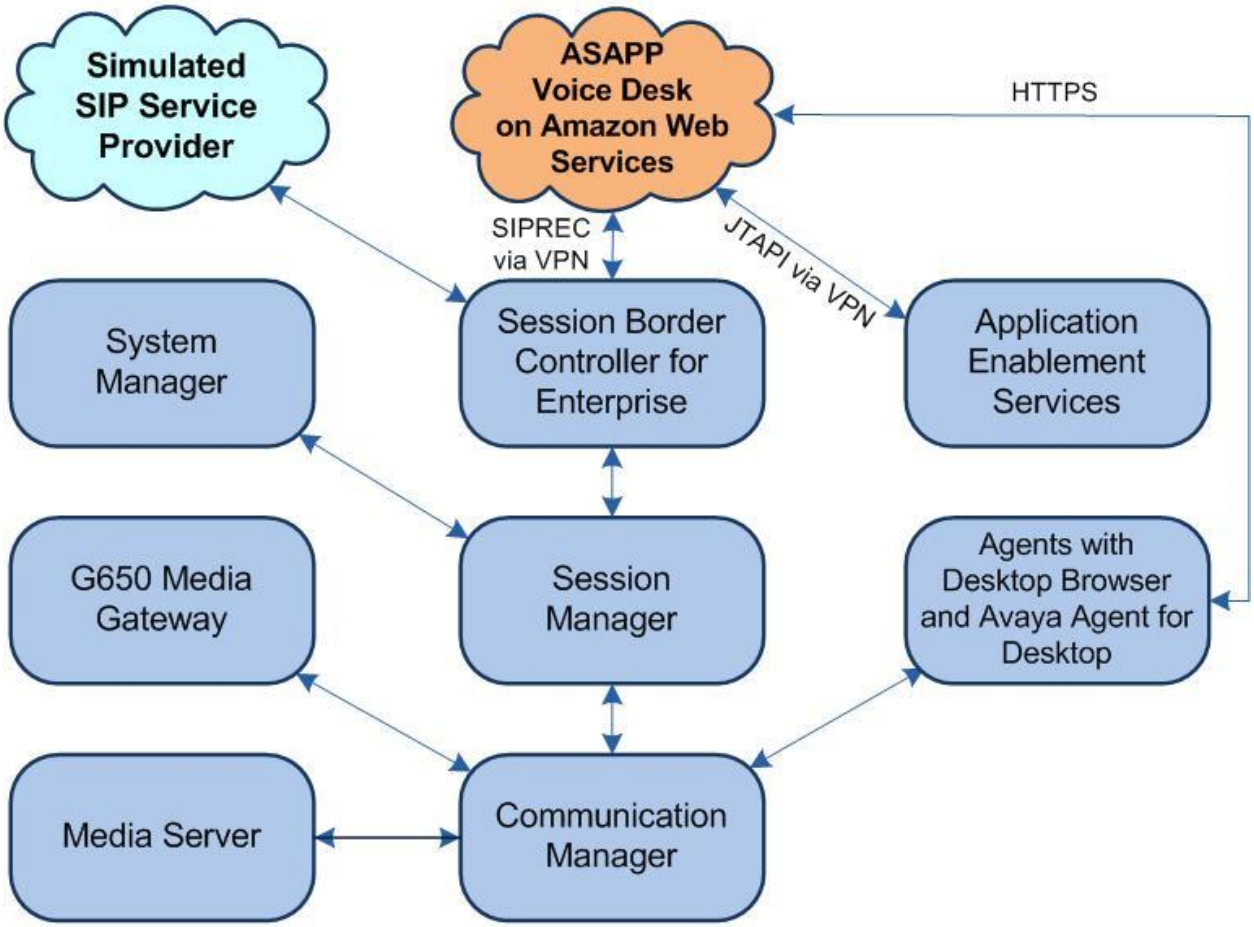


Figure 1: Compliance Testing Configuration

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 in Virtual Environment	8.1.3 (8.1.3.0.1.890.26685)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0 (8.0.2.138)
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3 (8.1.3.0.0.25-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.0.1012091)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.2 (8.1.2.0-31-19809)
Avaya Agent for Desktop (H.323)	2.0.6.0.10
ASAPP Voice Desk • CTI Adapter • Avaya JTAPI Windows Client • Media Gateway Proxies	2.2 2021-08-b36f736 8.1.3.0.0.25 2.0.4

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer CTI link
- Administer system parameters features
- Administer SIP trunk group
- Administer IP codec set

5.1. Verify License

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

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

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                         CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                           CAS Main? n
Answer Supervision by Call Classifier? y                  Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                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: 1
Extension: 60111
     Type: ADJ-IP
                                                                     COR: 1
     Name: AES CTI Link
Unicode Name? n
```

5.3. Administer System Parameters Features

Log into the System Access Terminal. 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: 27
```

Navigate to **Page 13** and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to ASAPP.

```
change system-parameters features                                Page  13 of  19
                        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? n
               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 SIP Trunk Group

Use the "**change trunk-group n**" command, where "**n**" is the trunk group number used by Communication Manager with Session Manager for calls with the PSTN. Enter the following values for the specified fields and retain the default values for the remaining fields.

In this case, the pertinent trunk group number is "**212**". Navigate to **Page 3**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **UUI Treatment:** "shared"
- **Send UCID:** "y"

```
add trunk-group 212                                                  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? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                 Modify Tandem Calling Number: no
               Send UCID? y



 Show ANSWERED BY on Display? y
```

5.5. Administer IP Codec Set

Use the "**change ip-codec-set n**" command, where "**n**" is an existing codec set number to be used by the agent stations. For **Audio Codec**, make certain that only a relevant variant of the G711 codec is configured, as required by ASAPP.

In the compliance testing, this codec was used by all agent stations.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
 3:
 4:
 5:
 6:
 7:

    Media Encryption                  Encrypted SRTP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: aes
 3: none
 4:
 5:
```

6. Configure Avaya Aura® Application Enablement Services

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

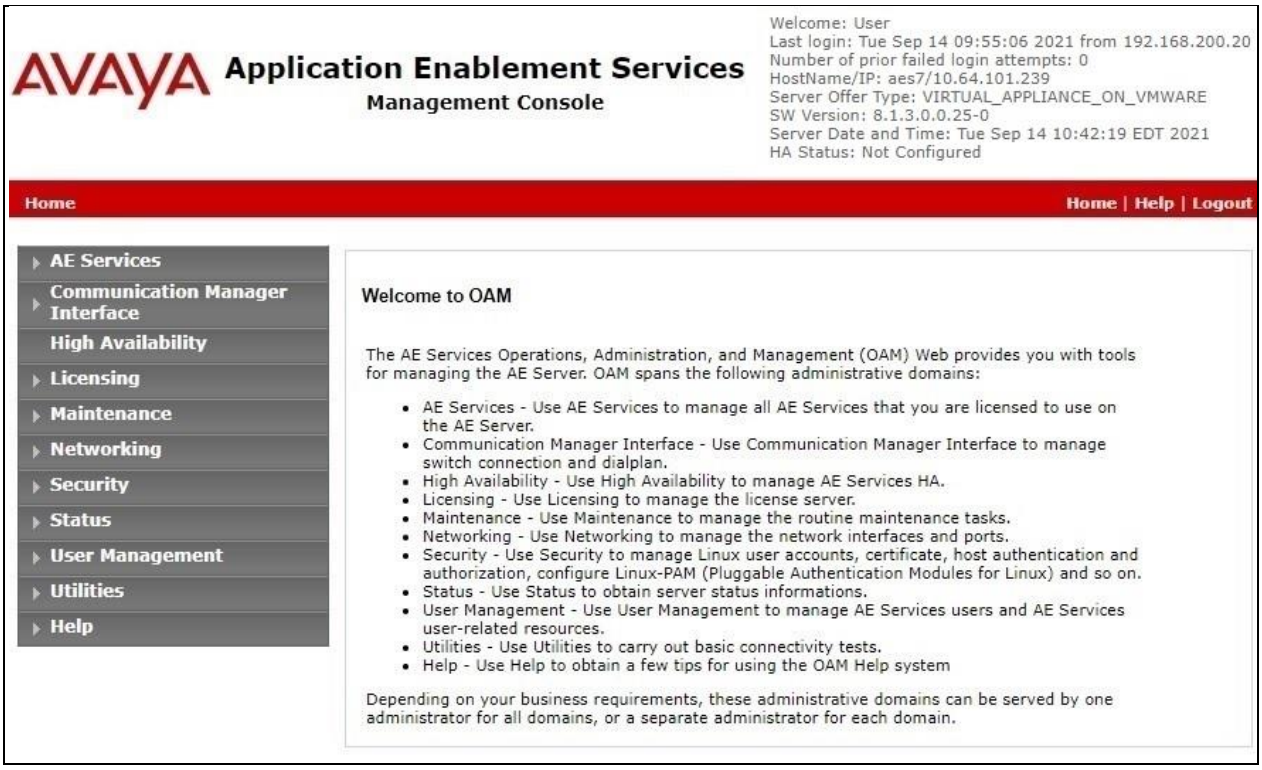
- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer ASAPP user
- Administer security database
- Administer ports
- Restart service
- Obtain Tlink name
- Export CA certificate

6.1. Launch OAM Interface

Access the OAM 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 screen below is displayed. Log in using the appropriate credentials.

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

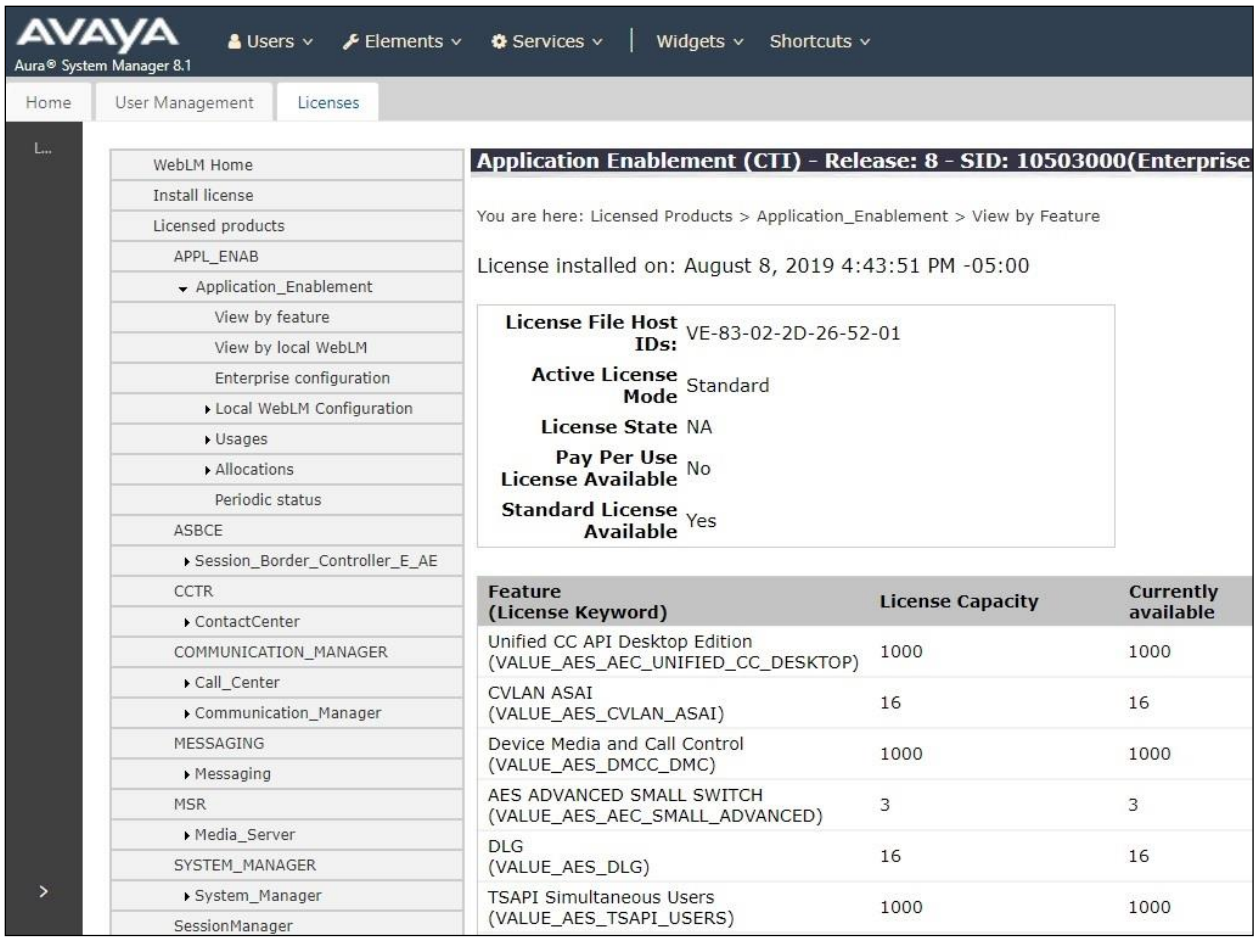


6.2. Verify License

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).

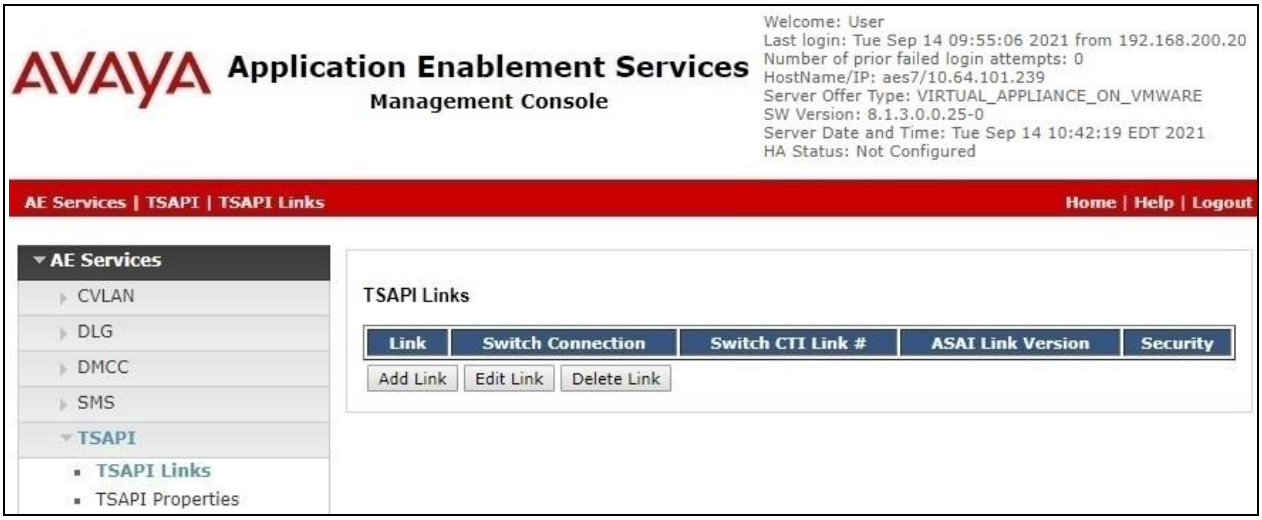
Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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



6.3. Administer TSAPI Link

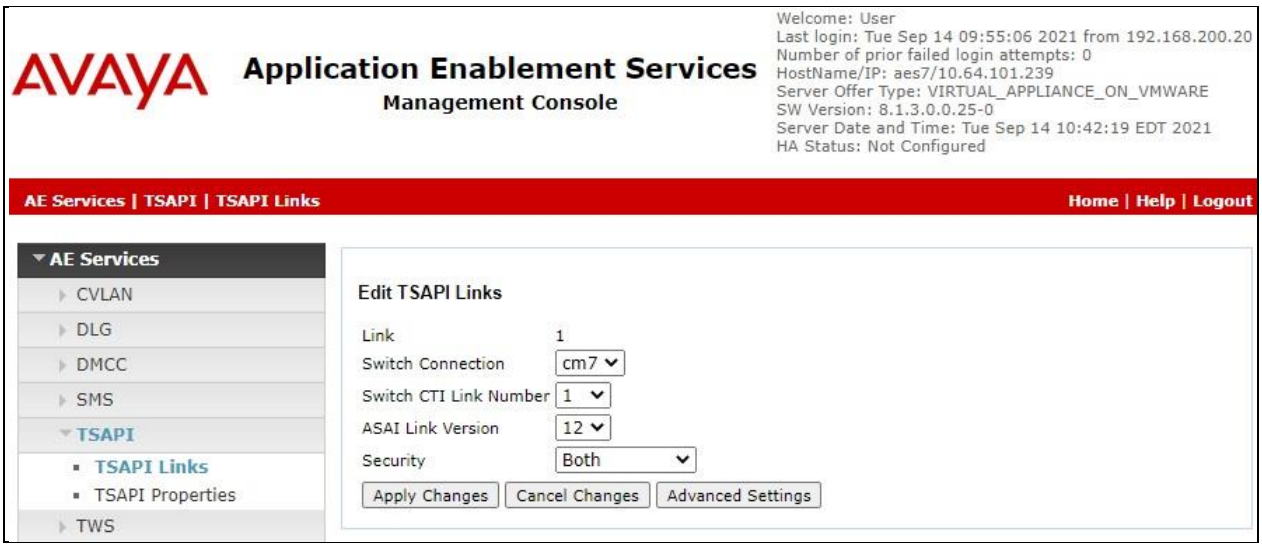
Select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console** to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



The **Add TSAPI Links** screen is displayed next. 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 "**cm7**". For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**.

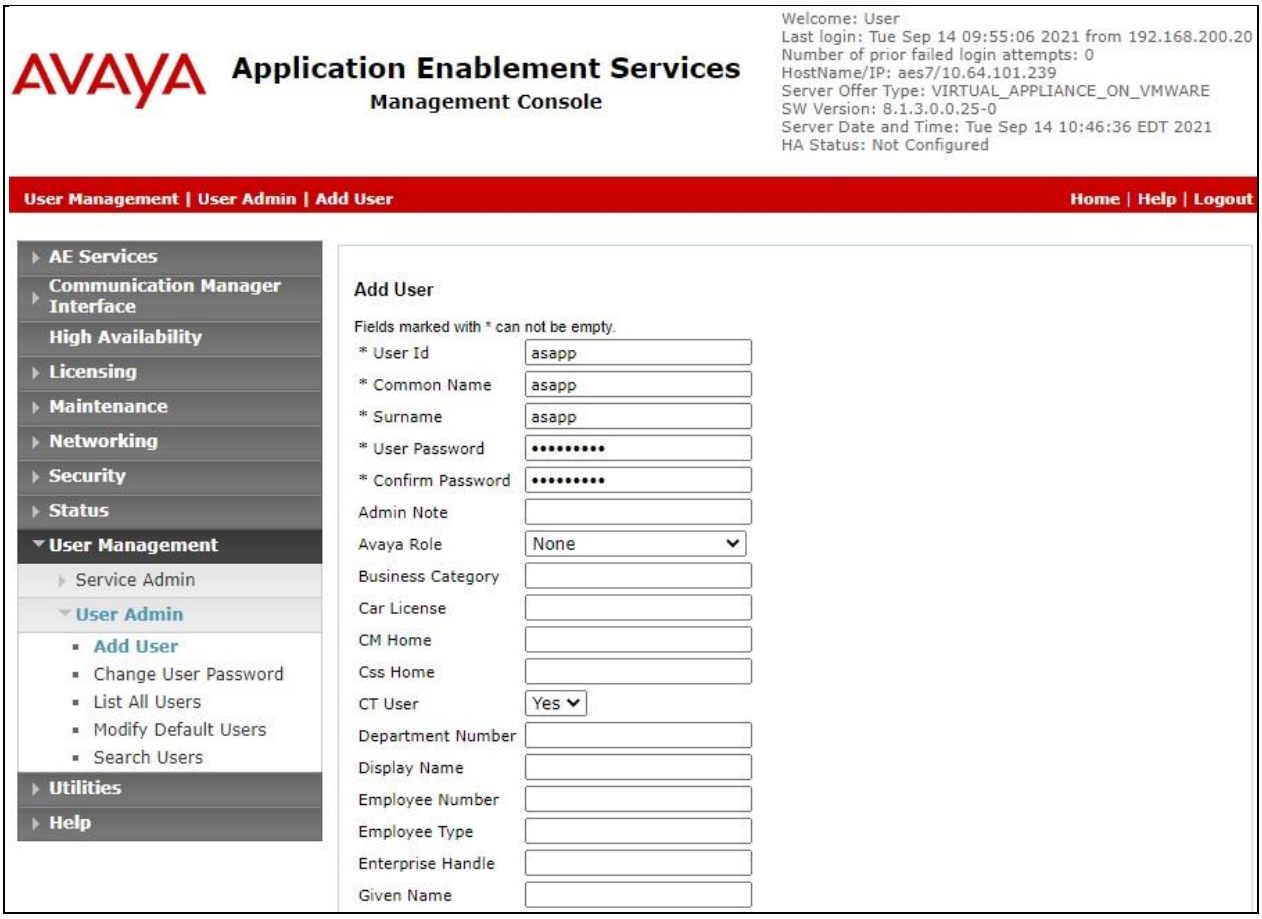
Retain the default value for **ASAI Link Version** and set **Security** to the desired value, in this case "**Both**" to allow for both encrypted and non-encrypted connections.



6.4. Administer ASAPP User

Select **User Management → User Admin → Add User** from the left pane, to display the **Add User** screen in the right pane.

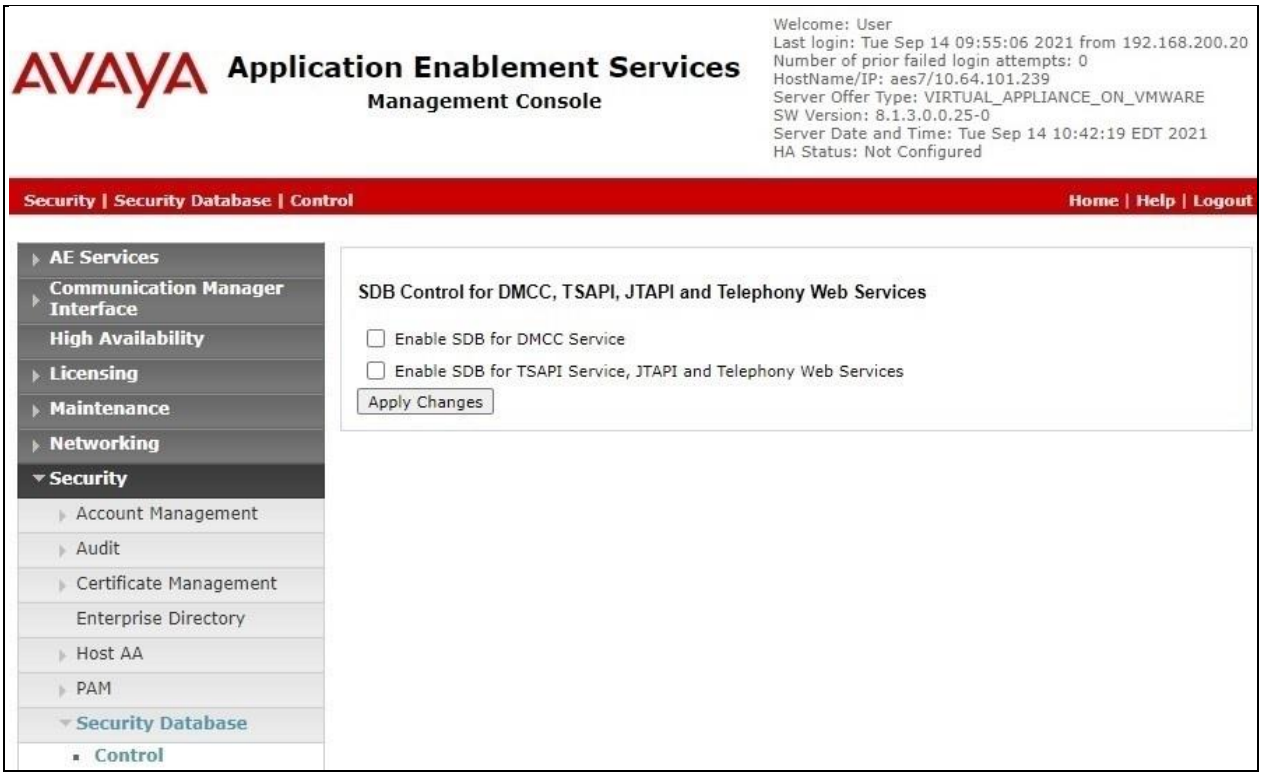
Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select "**Yes**" from the drop-down list. Retain the default value in the remaining fields.



6.5. Administer 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. Make certain both parameters are unchecked, as shown below.

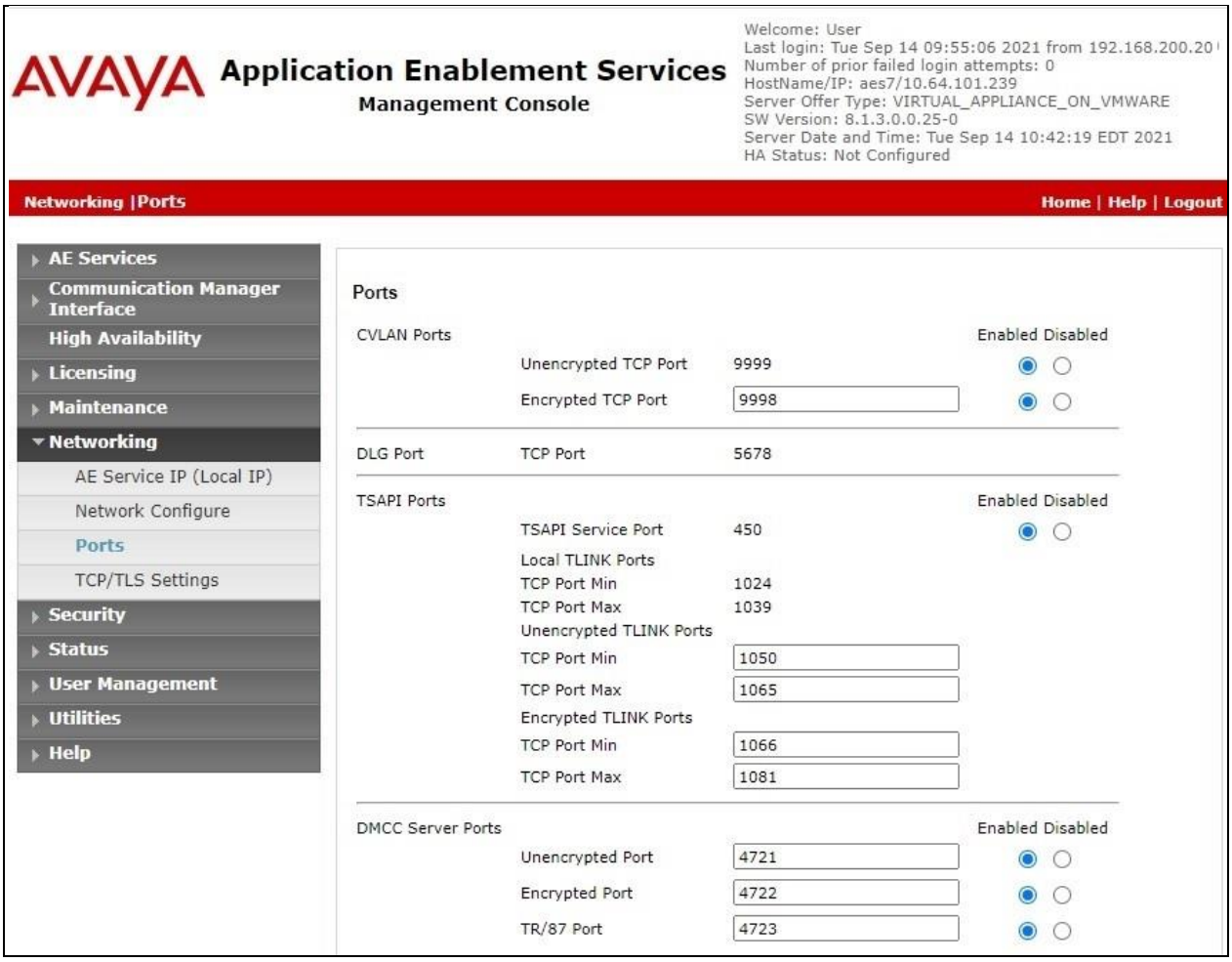
In the event that the security database is used by the customer with parameters already enabled, then follow reference [**2**] to configure access privileges for the ASAPP user from **Section 6.4**.



6.6. Administer Ports

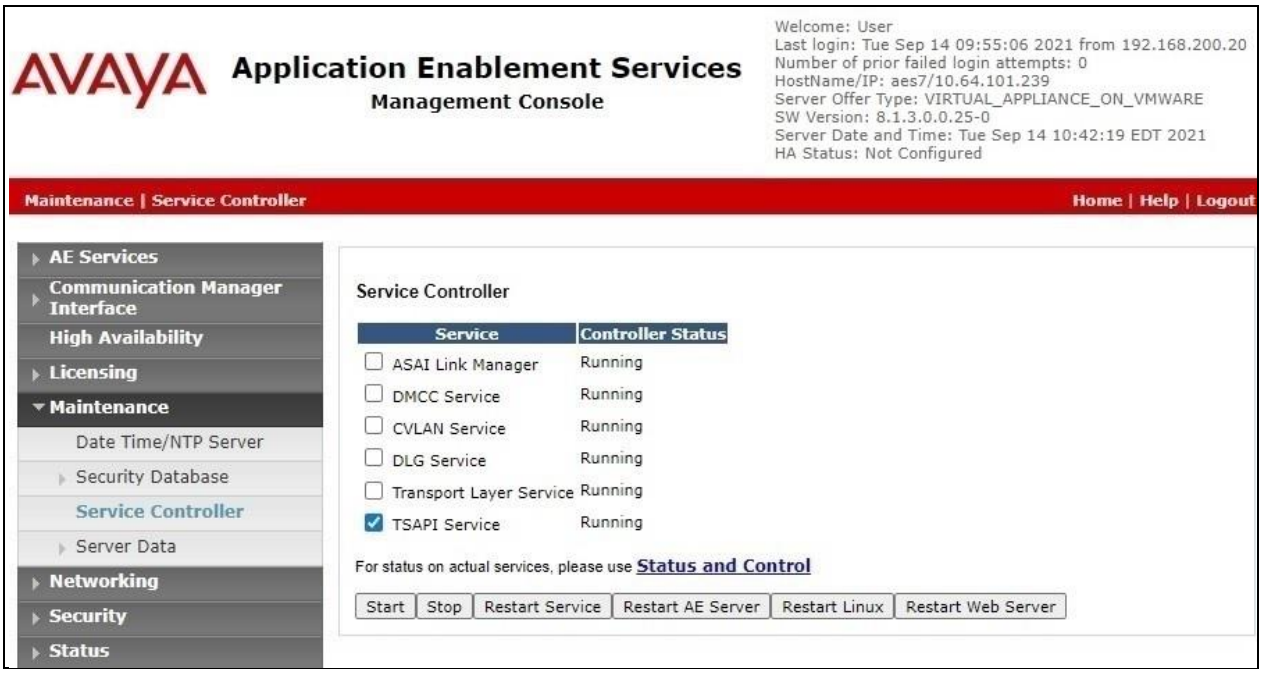
Select **Networking → Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **TSAPI Ports** section, make certain that **TSAPI Service Port** is **Enabled** as shown below. Retain the default values in the remaining fields.



6.7. Restart Service

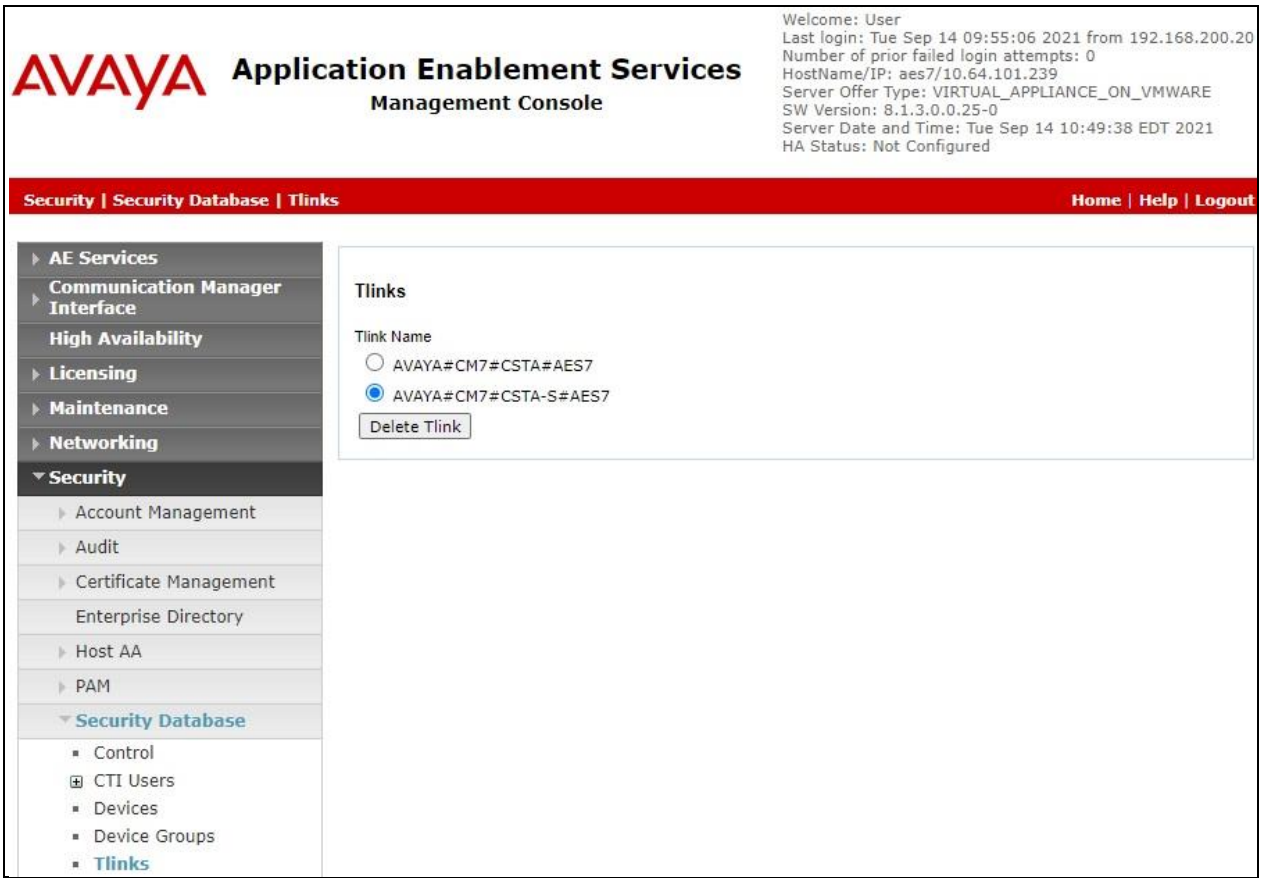
Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **TSAPI Service**. Select **Restart Service**.



6.8. Obtain Tlink Name

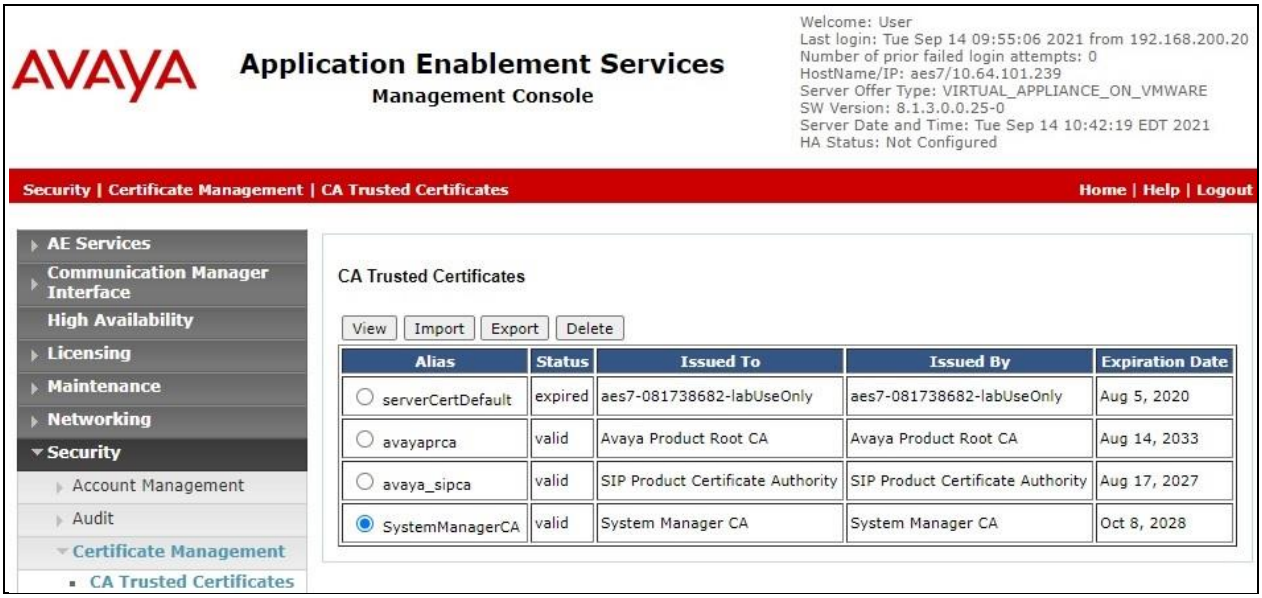
Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name.

Make a note of the pertinent Tlink name, to be used later to share with ASAPP. In this case, the pertinent Tlink name for encrypted connection is "**AVAYA#CM7#CSTA-S#AES7**", as shown below.

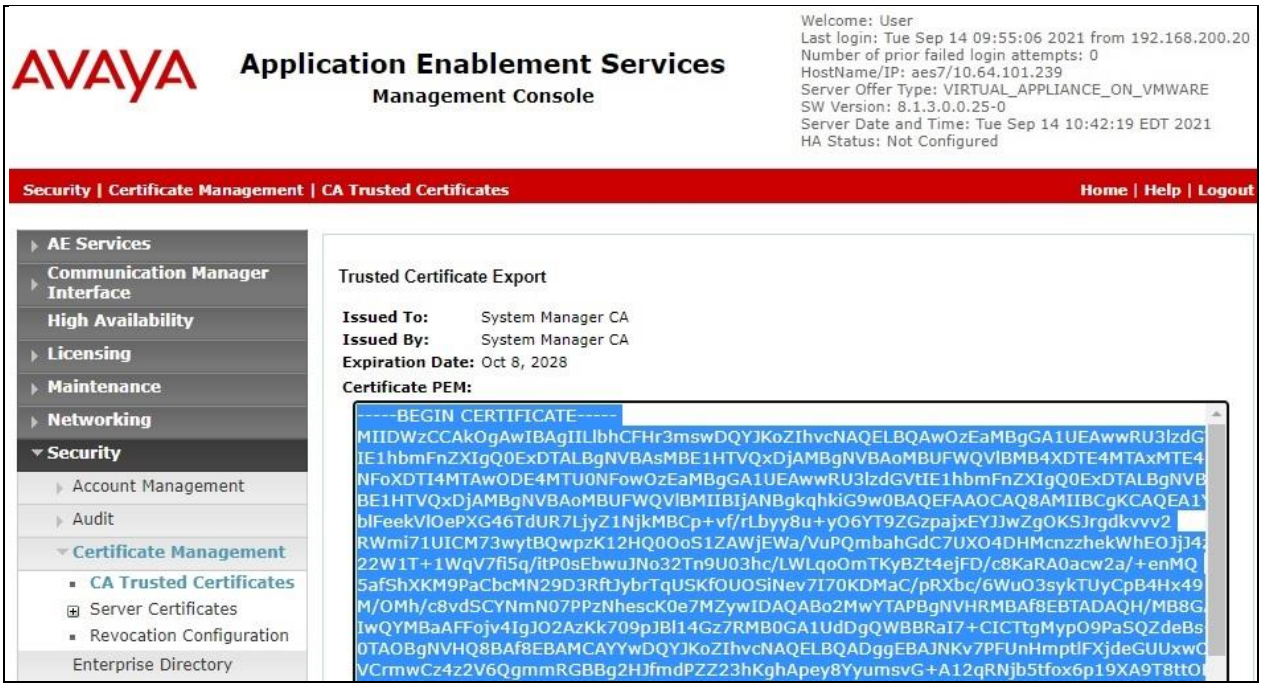


6.9. Export CA Certificate

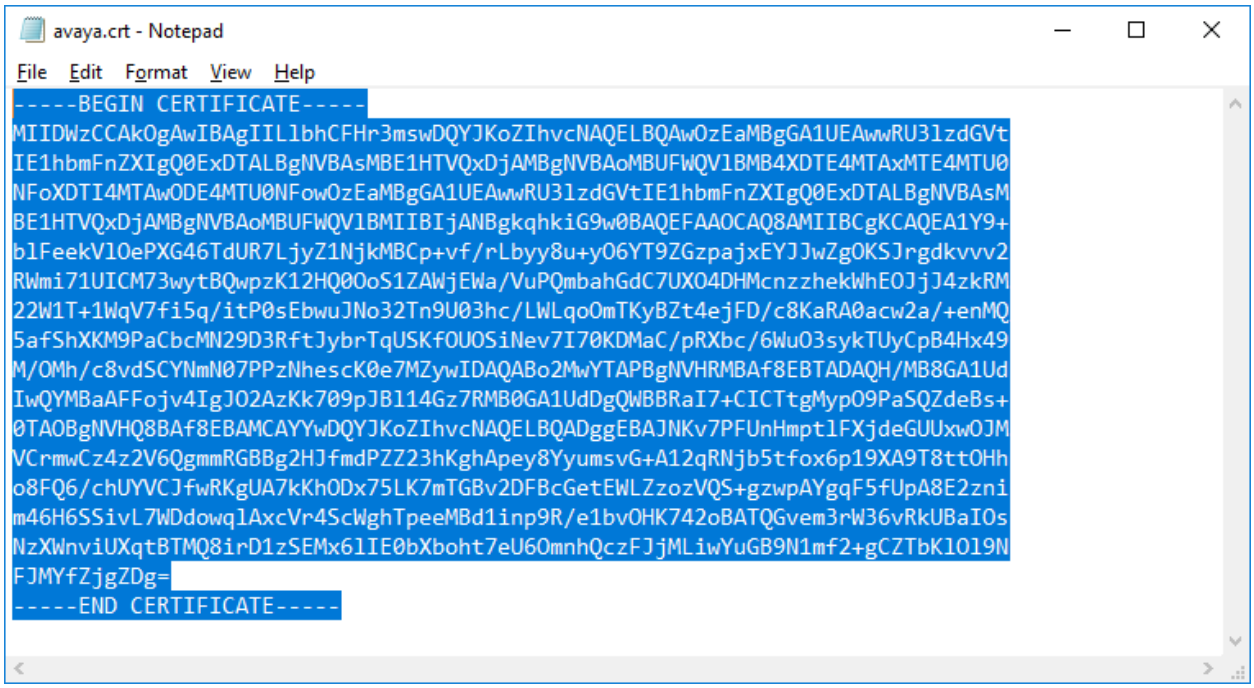
Select **Security → Certificate Management → CA Trusted Certificates** from the left pane, to display the **CA Trusted Certificates** screen. Select the pertinent CA certificate for secure connection with client applications, in this case "**SystemManagerCA**", and click **Export**.



The **Trusted Certificate Export** screen is displayed next. Copy everything in the text box, including the **BEGIN CERTIFICATE** and **END CERTIFICATE** (not shown) lines.



Paste the copied content to a Notepad file and save with a desired file name using **.crt** as suffix, such as **avaya.crt** in the compliance testing.




```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILlbhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBgGA1UEAwwRU3lzdGVt
IE1hbmFnZXIgQ0ExDTALBgNVBAsMBE1HTVQxDjAMBgNVBAoMBUFWQVlBMB4XDTE4MTAxMTE4MTU0
NFoXDTI4MTAwODE4MTU0NFowOzEaMBgGA1UEAwwRU3lzdGVtIE1hbmFnZXIgQ0ExDTALBgNVBAsM
BE1HTVQxDjAMBgNVBAoMBUFWQVlBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Y9+
blFeekVlOePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+yO6YT9ZGzpajxEYJJwZgOKSJrgdkvvv2
RWmi71UICM73wytBQwpzK12HQ0OoS1ZAWjEWa/VuPQmbahGdC7UXO4DHMcnzzhekWhEOJjJ4zkRM
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6WuO3sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud
IwQYMBaAFFojv4IgJO2AzKk709pJBl14Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMypO9PaSQZdeBs+
0TAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptlFXjdeGUUxwOJM
VCrmwCz4z2V6QgmmRGBBg2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8ttOHh
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zni
m46H6SSivL7WDdowqlAxcVr4ScWghTpeeMBd1inp9R/e1bvOHK742oBATQGvem3rW36vRkUBaIOs
NzXWnviUXqtBTMQ8irD1zSEMx6lIE0bXboht7eU6OmnhQczFJjMLiwYuGB9N1mf2+gCZTbKlOl9N
FJMYfZjgZDg=
-----END CERTIFICATE-----
```

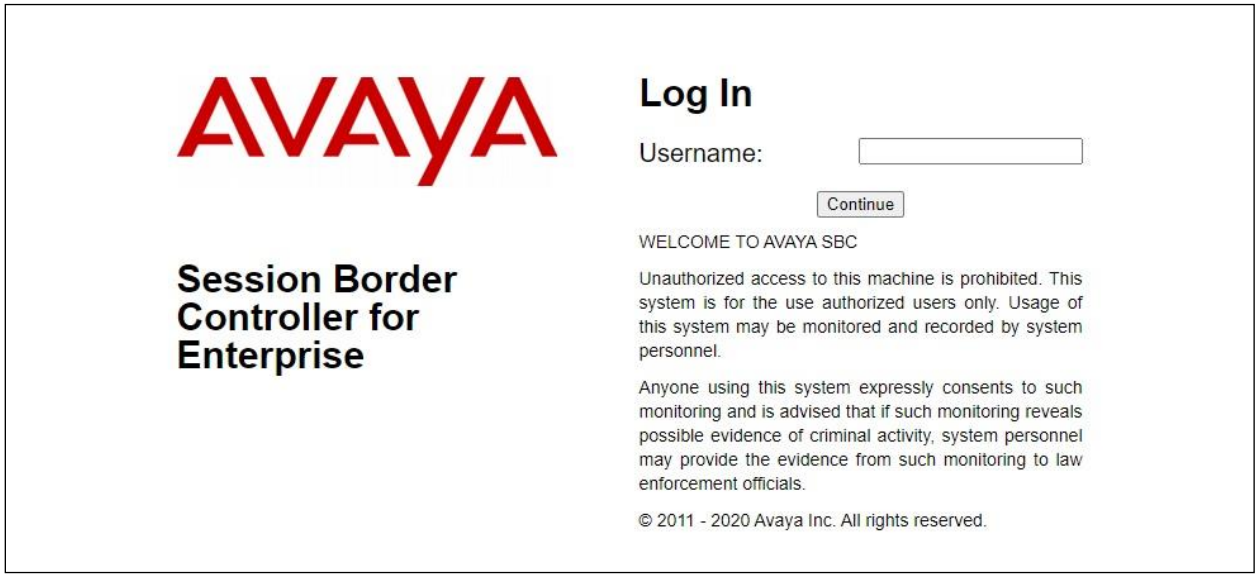
7. Configure Avaya Session Border Controller for Enterprise

This section provides the procedures for configuring SBCE. The procedures include the following areas:

- Launch web interface
- Administer SIP servers
- Administer routing
- Administer signaling rules
- Administer end point policy groups
- Administer recording profile
- Administer session policies
- Administer session flows
- Administer end point flows

7.1. Launch Web Interface

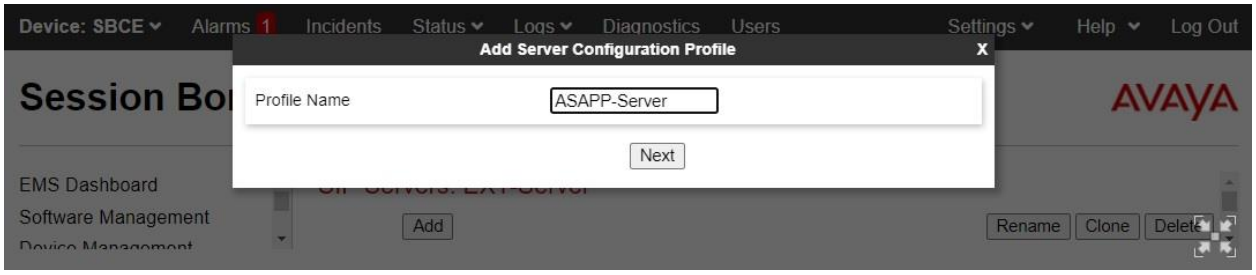
Access the SBCE web interface by using the URL "**https://ip-address/sbc**" in an Internet browser window, where "**ip-address**" is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.



7.2. Administer SIP Servers

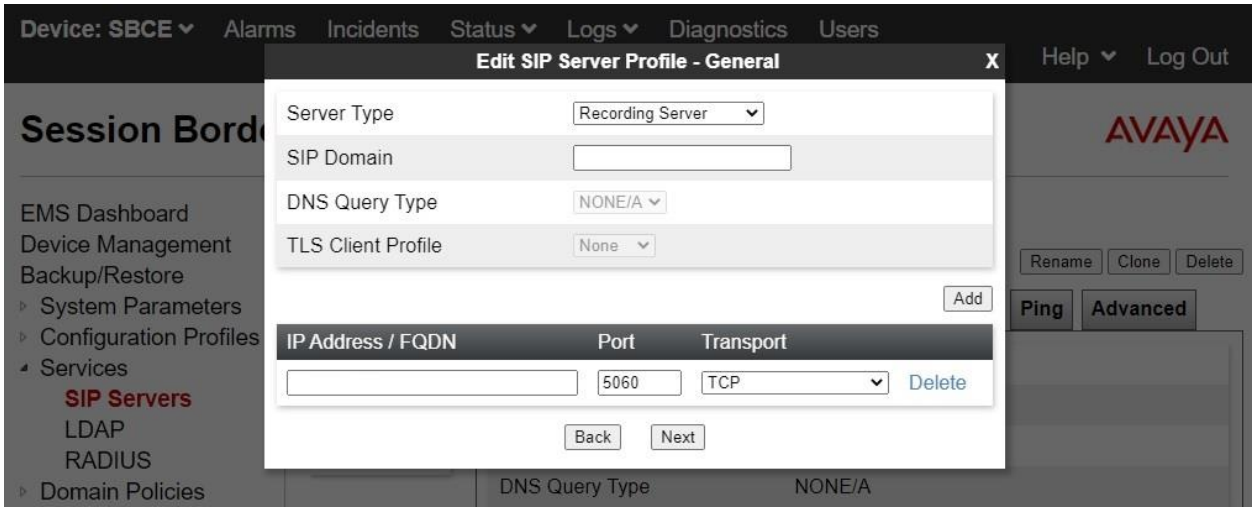
In the subsequent screen, select **Device → SBCE** from the top menu, followed by **Backup/Restore → Services → SIP Servers** from the left pane to display existing SIP server profiles. Click **Add** to add a SIP server profile for ASAPP.

The **Add Server Configuration Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.

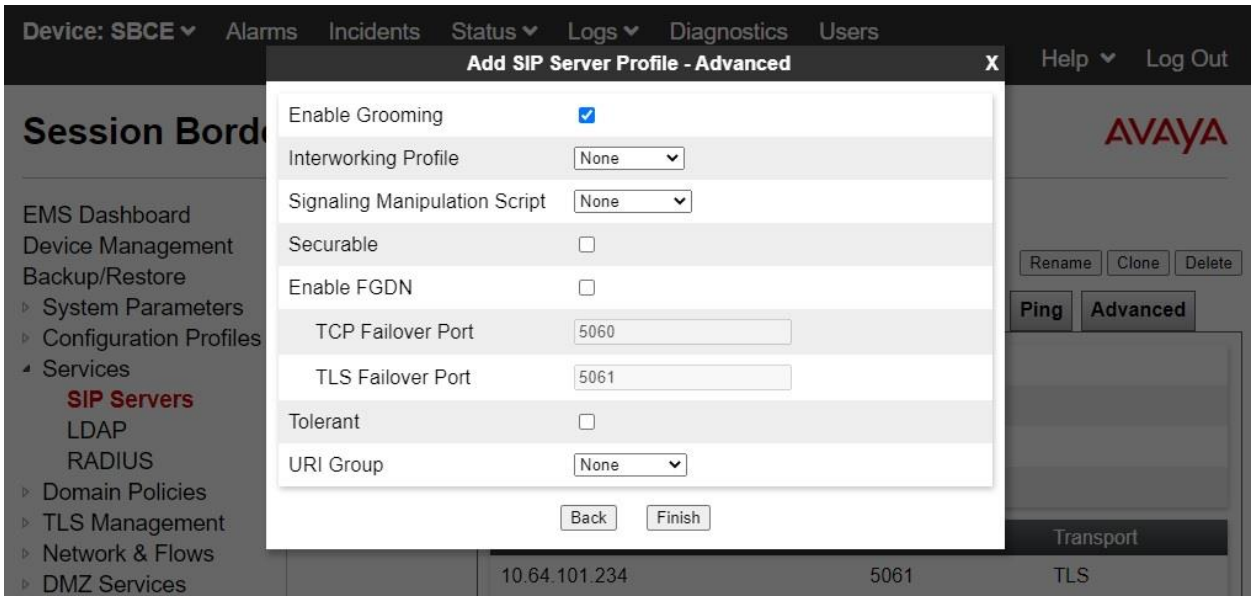


The **Edit SIP Server Profile – General** pop-up screen is displayed. Click **Add** to add an entry and enter the following values for the specified fields and retain the default values for the remaining fields.

- **Server Type:** "Recording Server"
- **IP Address / FQDN:** IP address of ASAPP Media Gateway Proxies (not shown below).
- **Port:** "5060"
- **Transport:** "TCP"

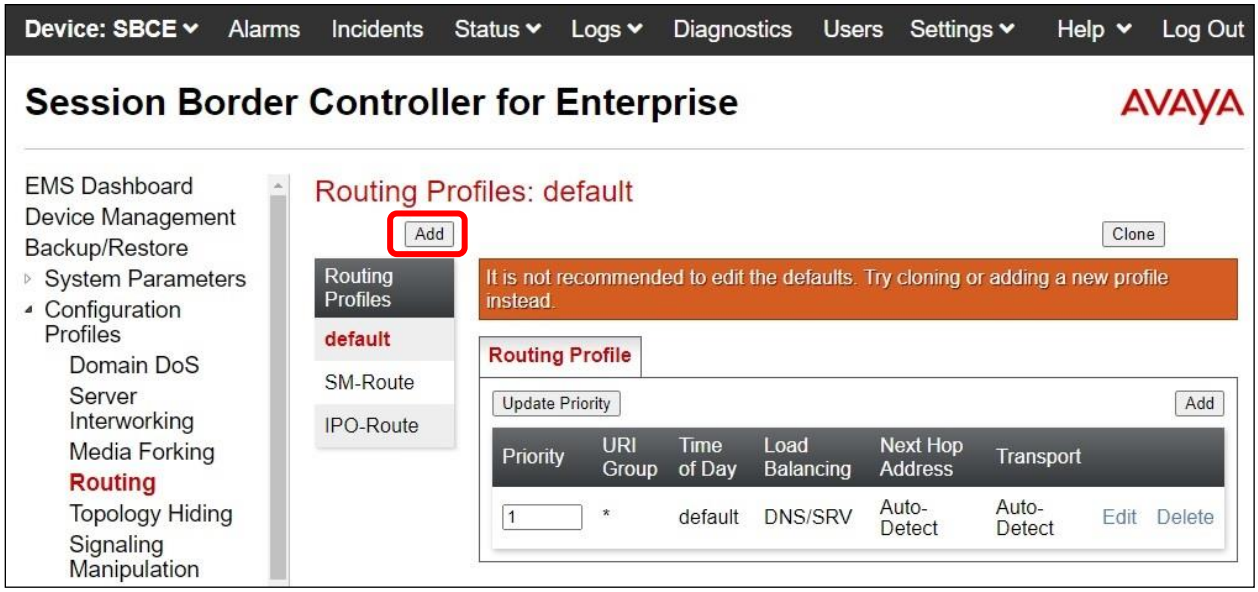


Navigate to the **Add SIP Server Profile - Advanced** screen. Retain the check in **Enable Grooming** and the default values in the remaining fields.

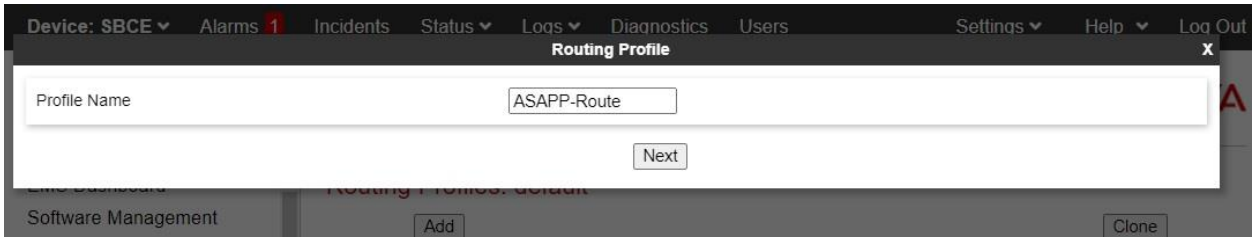


7.3. Administer Routing

Select **Backup/Restore → Configuration Profiles → Routing** from the left pane to display existing routing profiles. Click **Add** to add a routing profile for ASAPP.

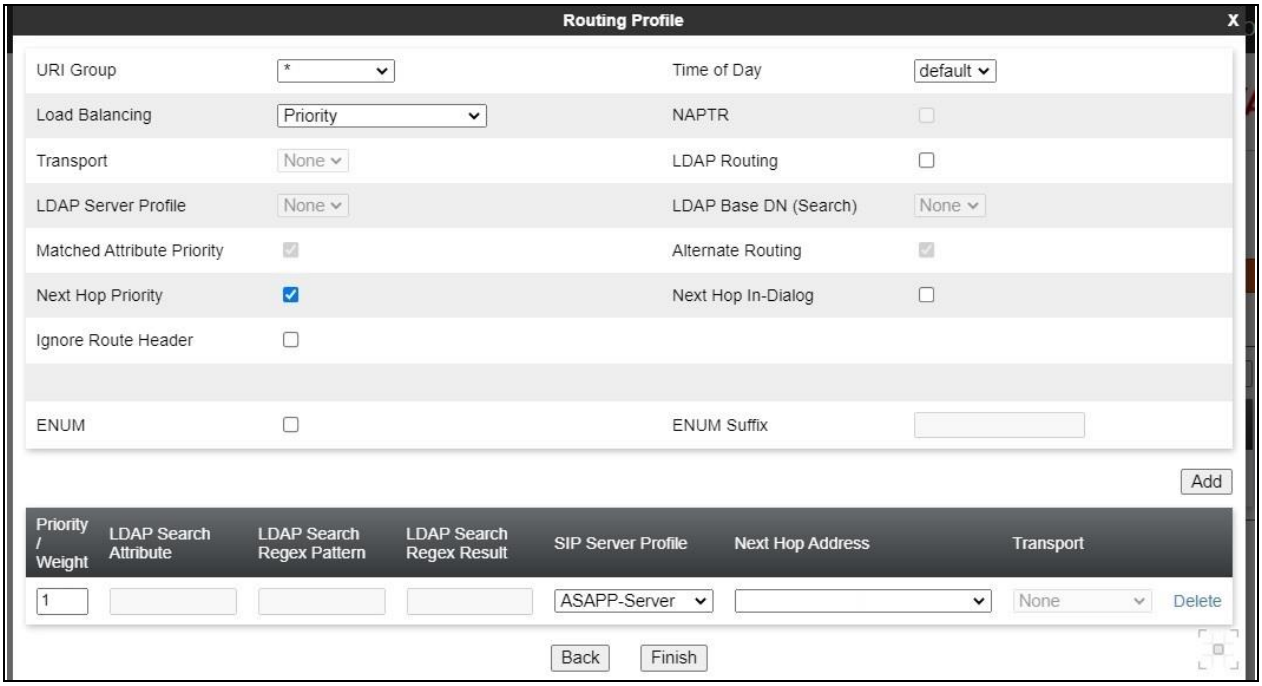


The **Routing Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.



The **Routing Profile** pop-up screen is updated as shown below. Click **Add** to add a next hop entry. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Priority / Weight:** The highest priority of "1".
- **SIP Server Profile:** Select the ASAPP SIP server profile from **Section 7.2**.
- **Next Hop Address:** Retain the auto populated value (not shown below).



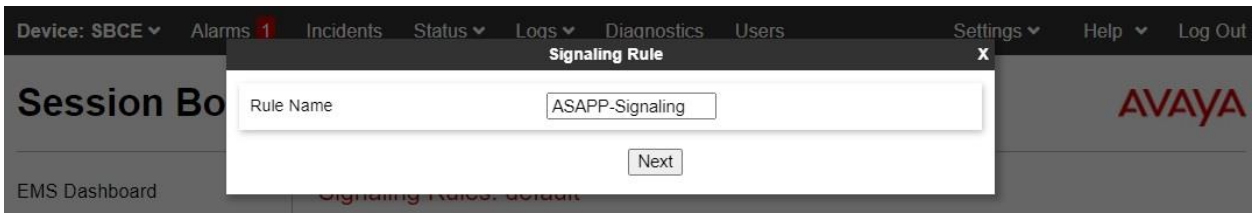
7.4. Administer Signaling Rules

Select **Backup/Restore → Domain Policies → Signaling Rules** from the left pane to display existing signaling rules.

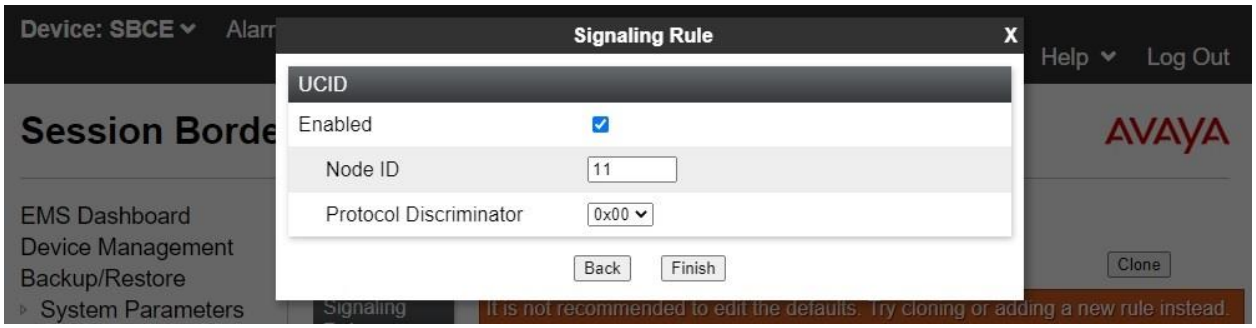
7.4.1. ASAPP Signaling Rule

Click **Add** to add a signaling rule for ASAPP.

The **Signaling Rule** pop-up screen is displayed. Enter a desired **Rule Name** as shown below.

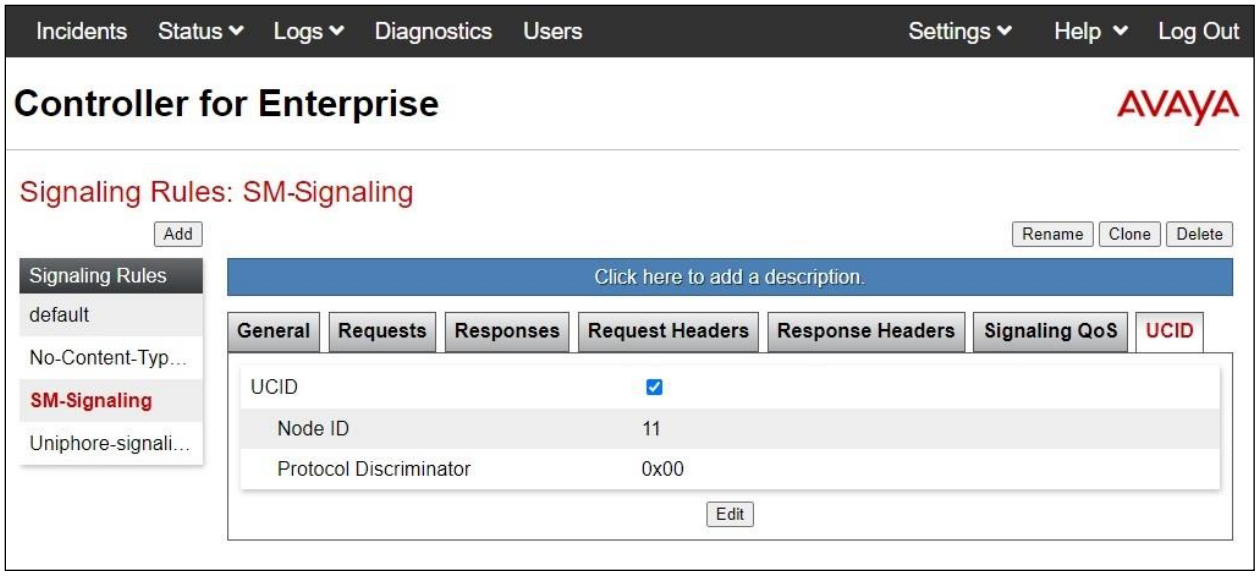


The **Signaling Rule** pop-up screen is updated. Navigate to the **UCID** page. Check **Enabled**. For **Node ID**, set this to the same value as the Session Manager signaling rule in **Section 7.4.2**, in this case "**11**" as shown below. Retain the default value in the remaining field.



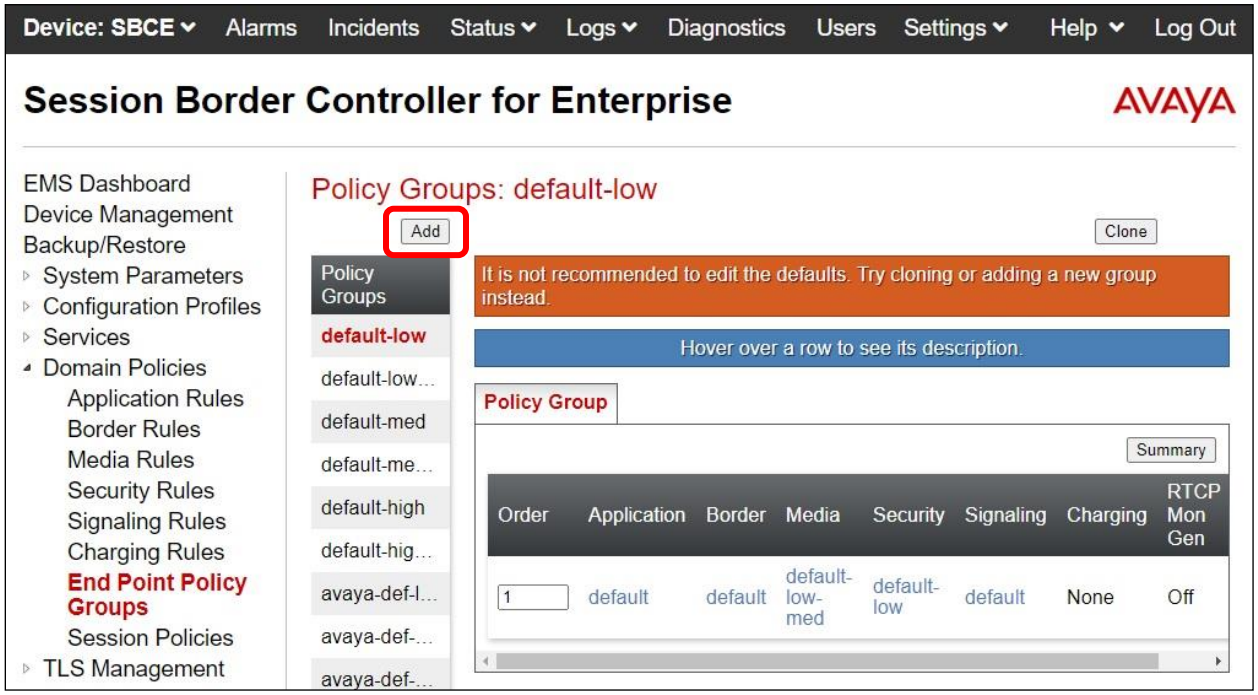
7.4.2. Session Manager Signaling Rule

Select the existing signaling rule for Session Manager, in this case **SM-Signaling**. Select the **UCID** tab. Make certain that **UCID** is checked, and that **Node ID** is configured with a unique number across the customer system, as shown below.

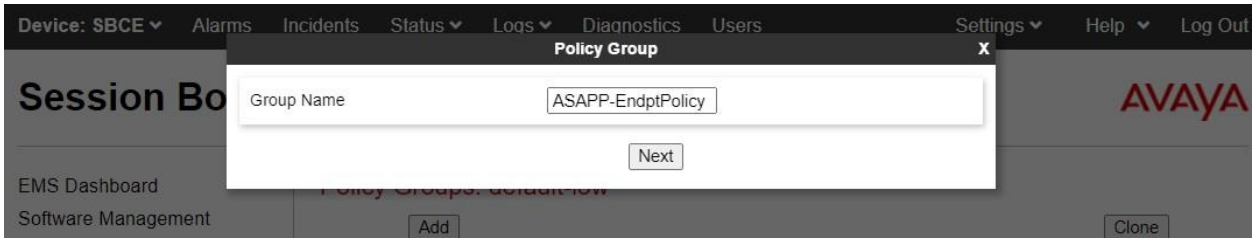


7.5. Administer End Point Policy Groups

Select **Backup/Restore → Domain Policies → End Point Policy Groups** from the left pane to display existing policy groups. Click **Add** to add a policy group for ASAPP.

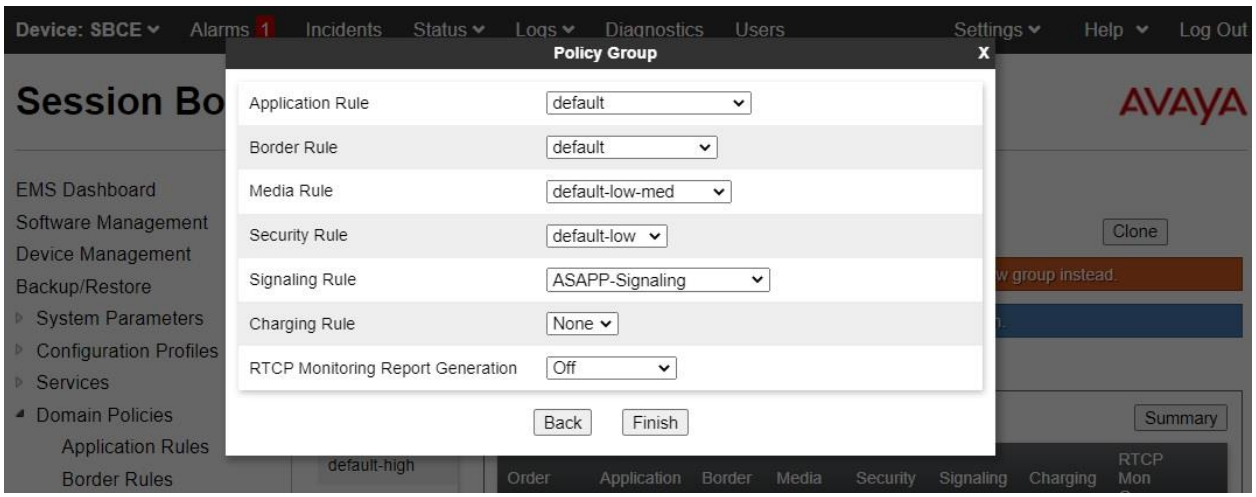


The **Policy Group** pop-up screen is displayed. Enter a desired **Group Name** as shown below.



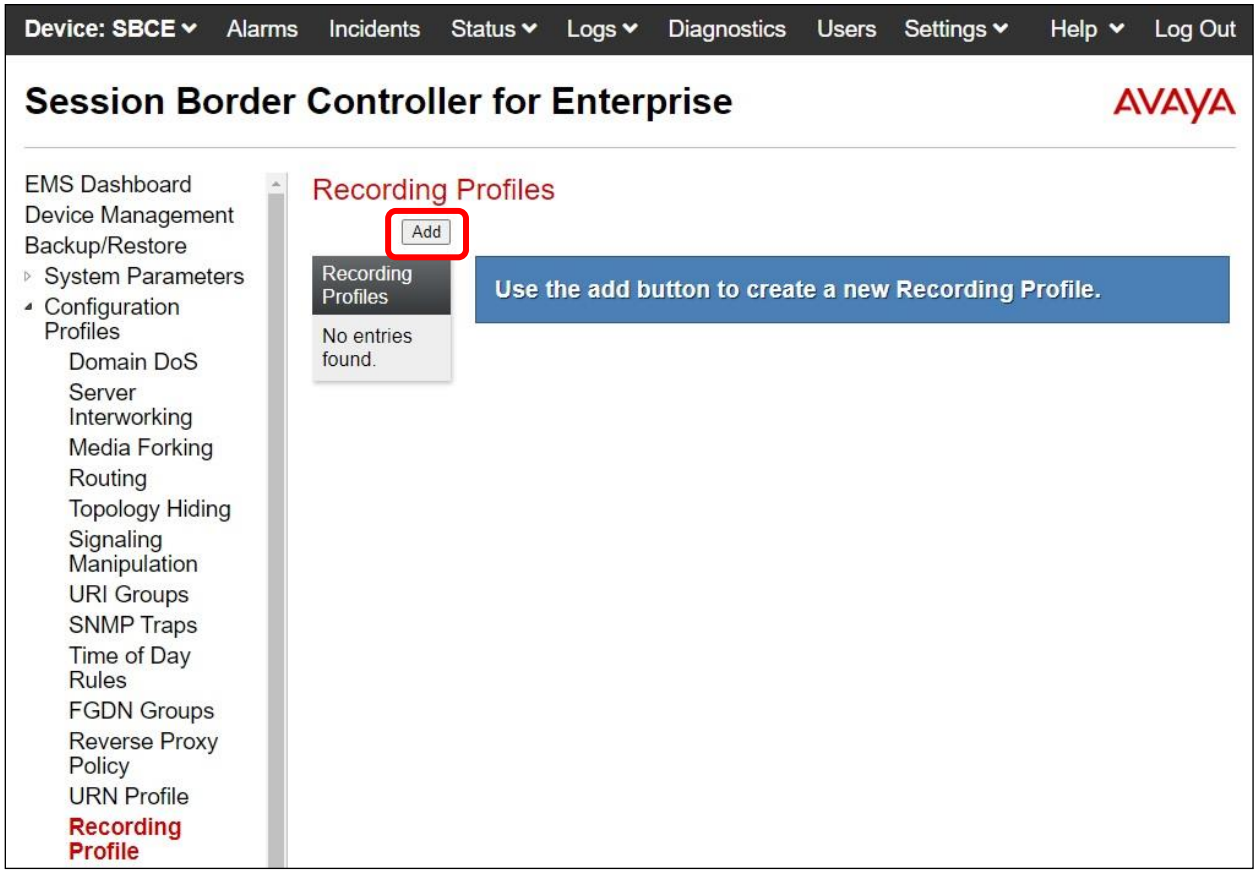
The **Policy Group** pop-up screen is updated as shown below. For **Signaling Rule**, select the ASAPP signaling rule from **Section 7.4.1**.

Retain the default values for the remaining fields.

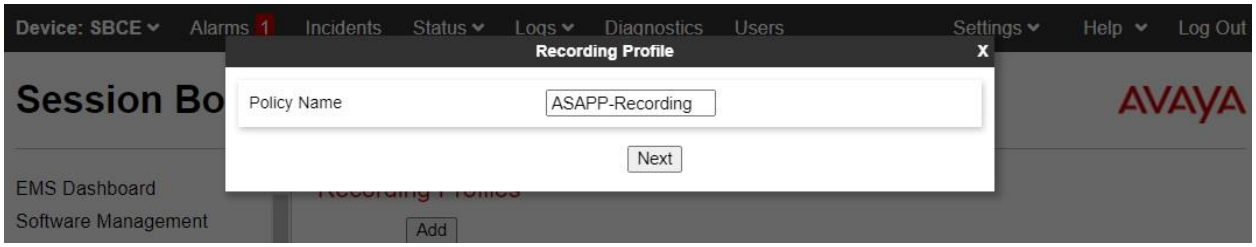


7.6. Administer Recording Profile

Select **Backup/Restore → Configuration Profiles → Recording Profile** from the left pane to display existing recording profiles. Click **Add** to add a recording profile for ASAPP.

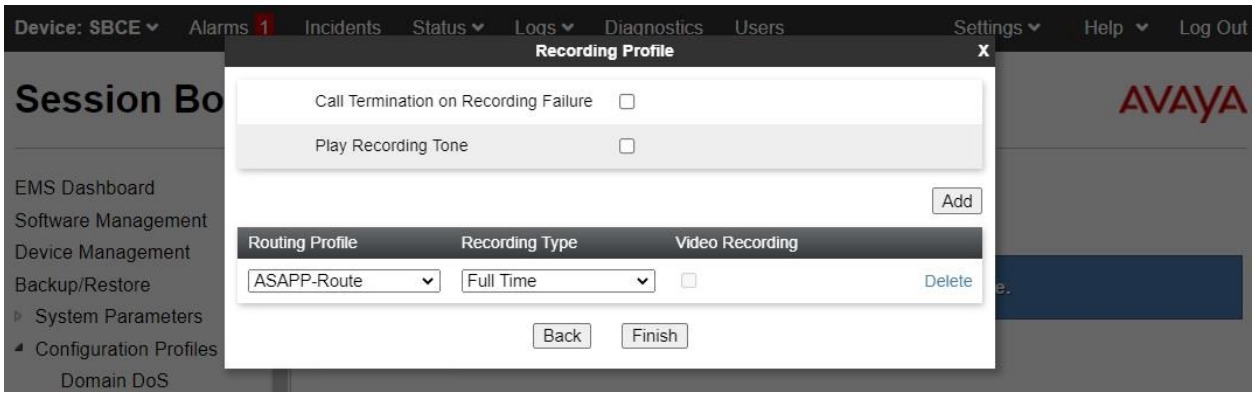


The **Recording Profile** pop-up screen is displayed. Enter a desired **Policy Name** as shown below.



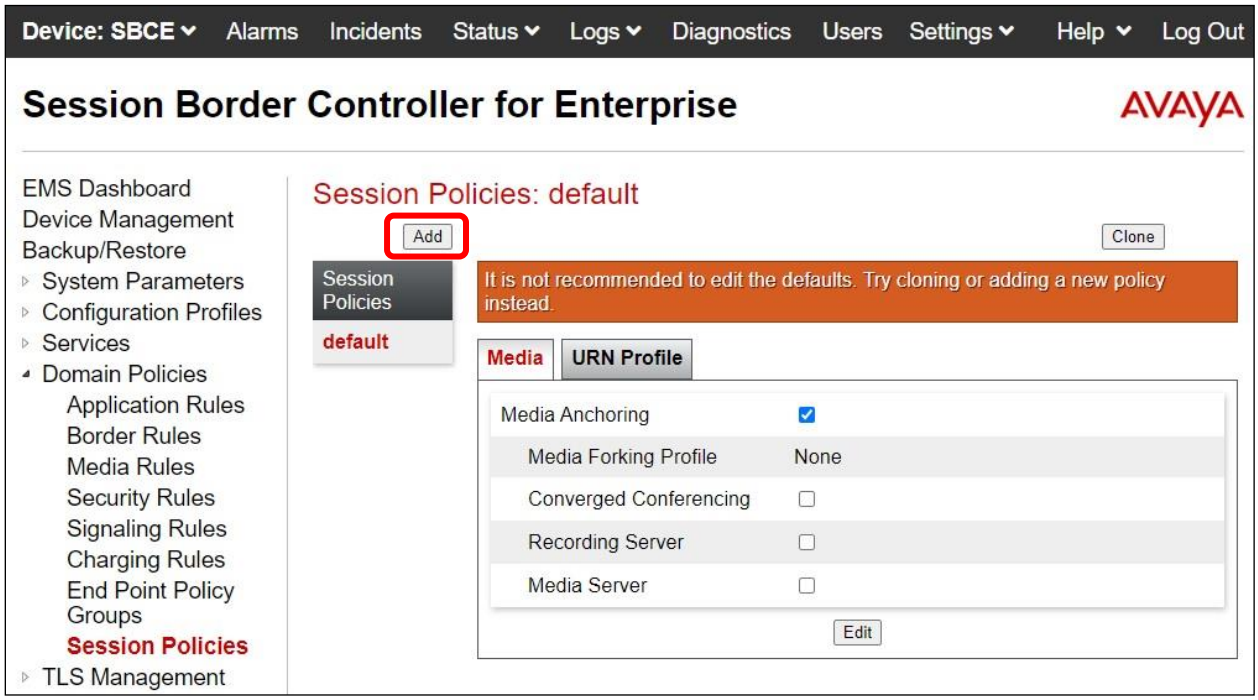
The **Recording Profile** pop-up screen is displayed as shown below. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Play Recording Tone:** Check this field if customer desires recording tone to be played.
- **Routing Profile:** Select the ASAPP routing profile from **Section 7.3**.
- **Recording Type:** "Full Time"

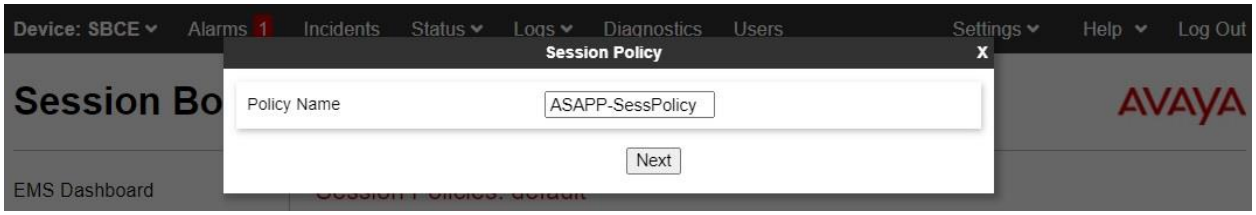


7.7. Administer Session Policies

Select **Backup/Restore → Domain Policies → Session Policies** from the left pane to display existing session policies. Click **Add** to add a session policy for ASAPP.

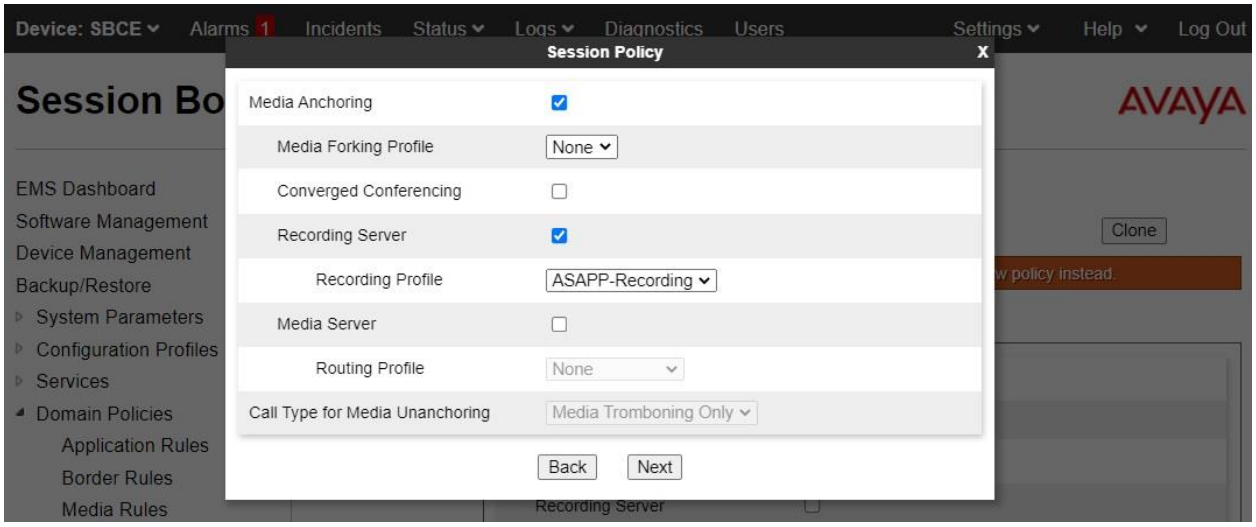


The **Session Policy** pop-up screen is displayed. Enter a desired **Policy Name** as shown below.



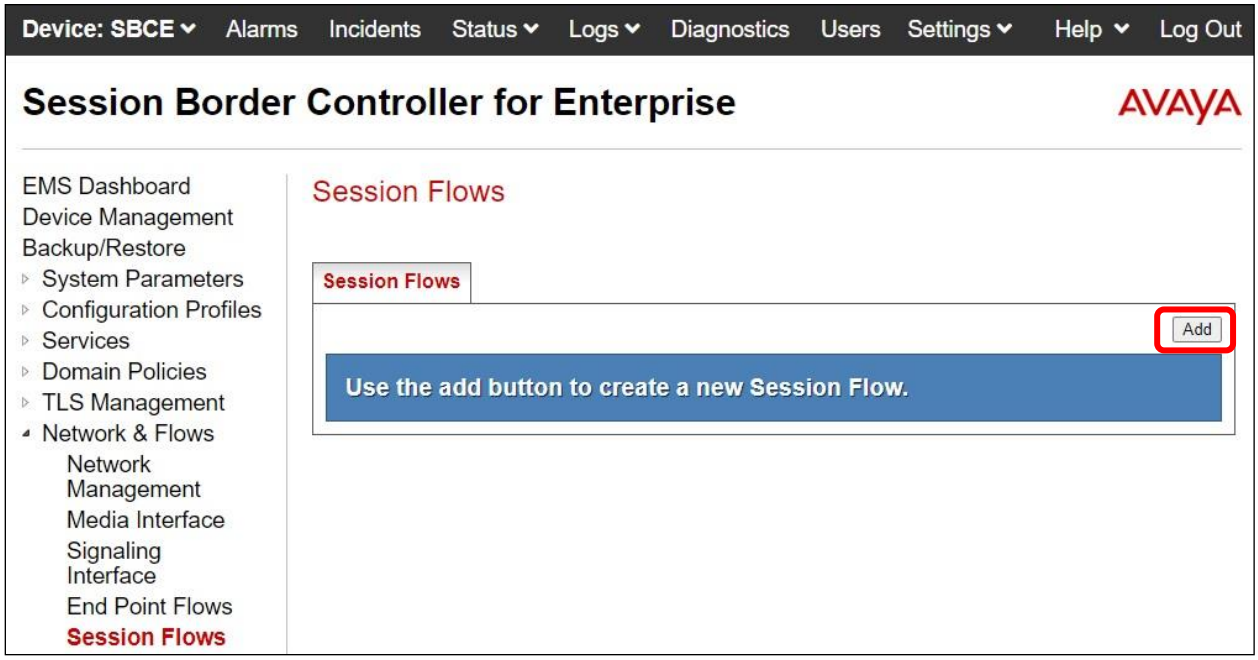
The **Session Policy** pop-up screen is updated as shown below. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Media Anchoring:** Check this field.
- **Recording Server:** Check this field.
- **Recording Profile:** Select the ASAPP recording profile from **Section 7.6**.

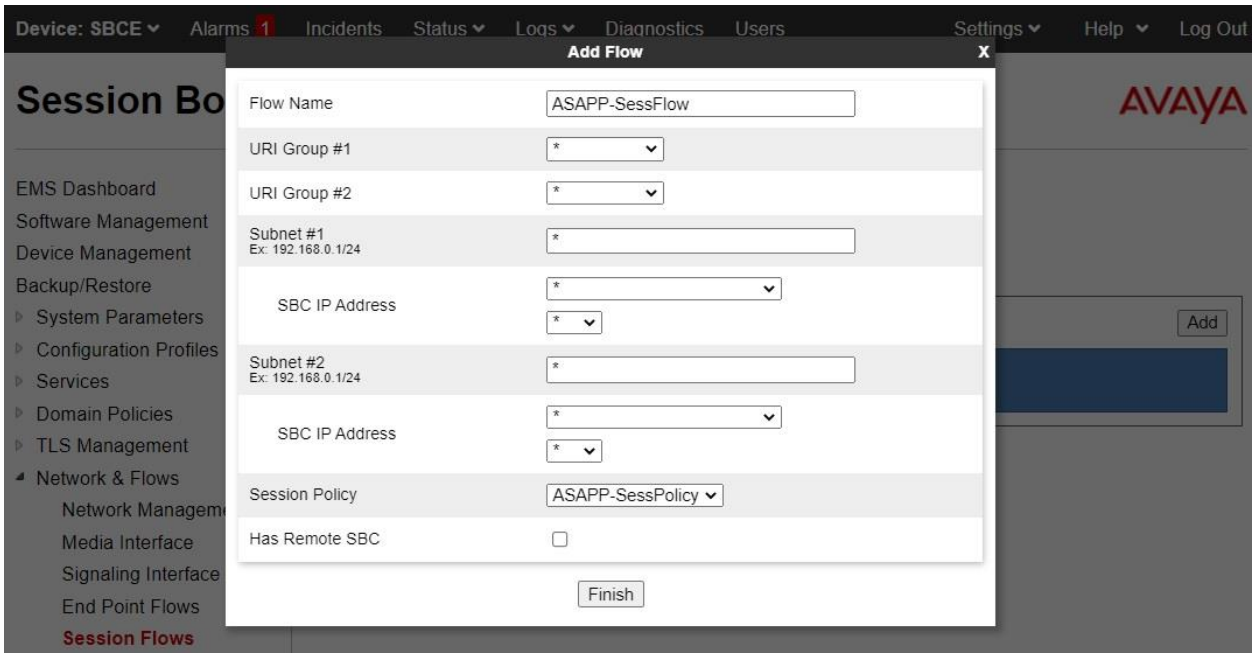


7.8. Administer Session Flows

Select **Backup/Restore → Network & Flows → Session Flows** from the left pane to display existing session flows. Click **Add** to add a session flow for ASAPP.

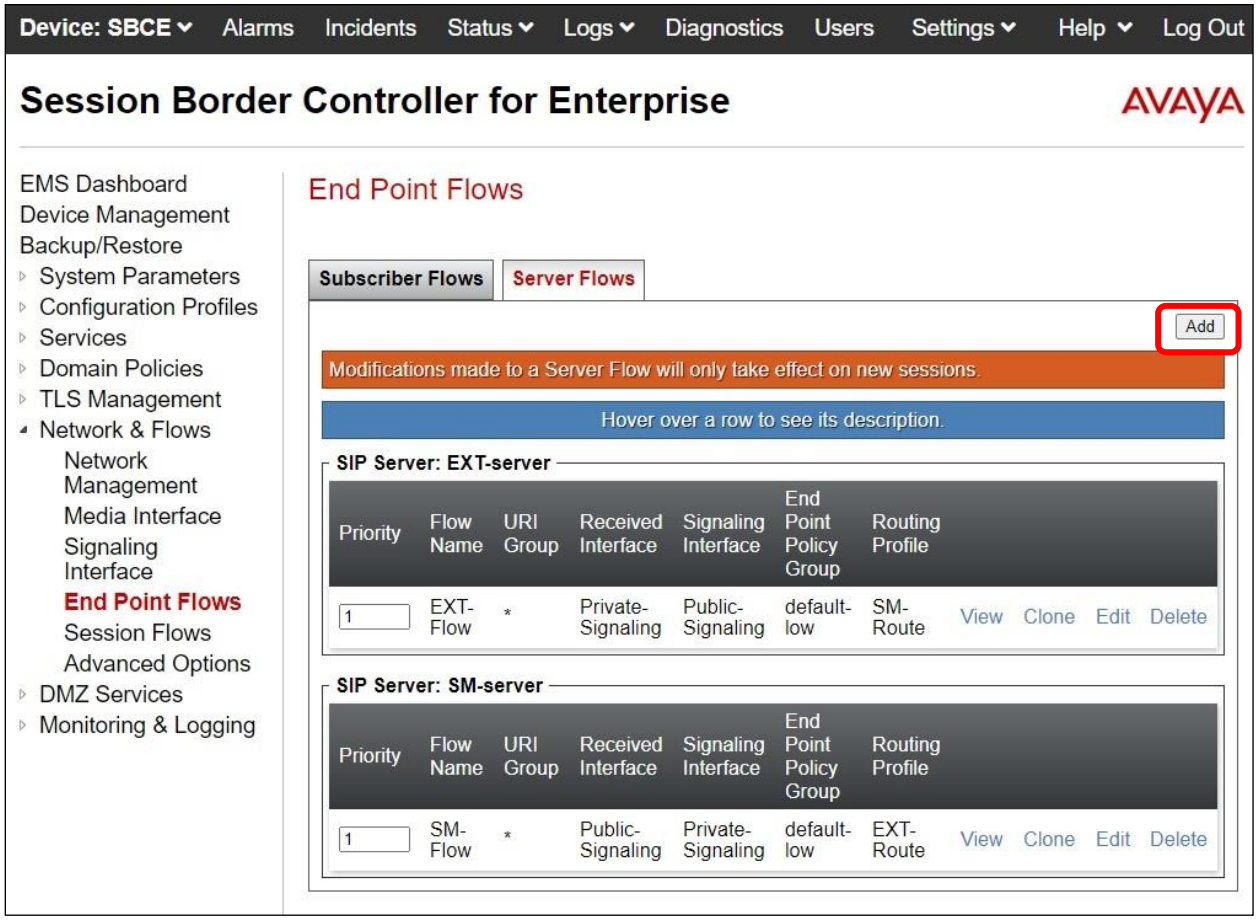


The **Add Flow** pop-up screen is displayed. For **Flow Name**, enter a desired name. For **Session Policy**, select the ASAPP session policy from **Section 7.7**. Retain the default values in the remaining fields.



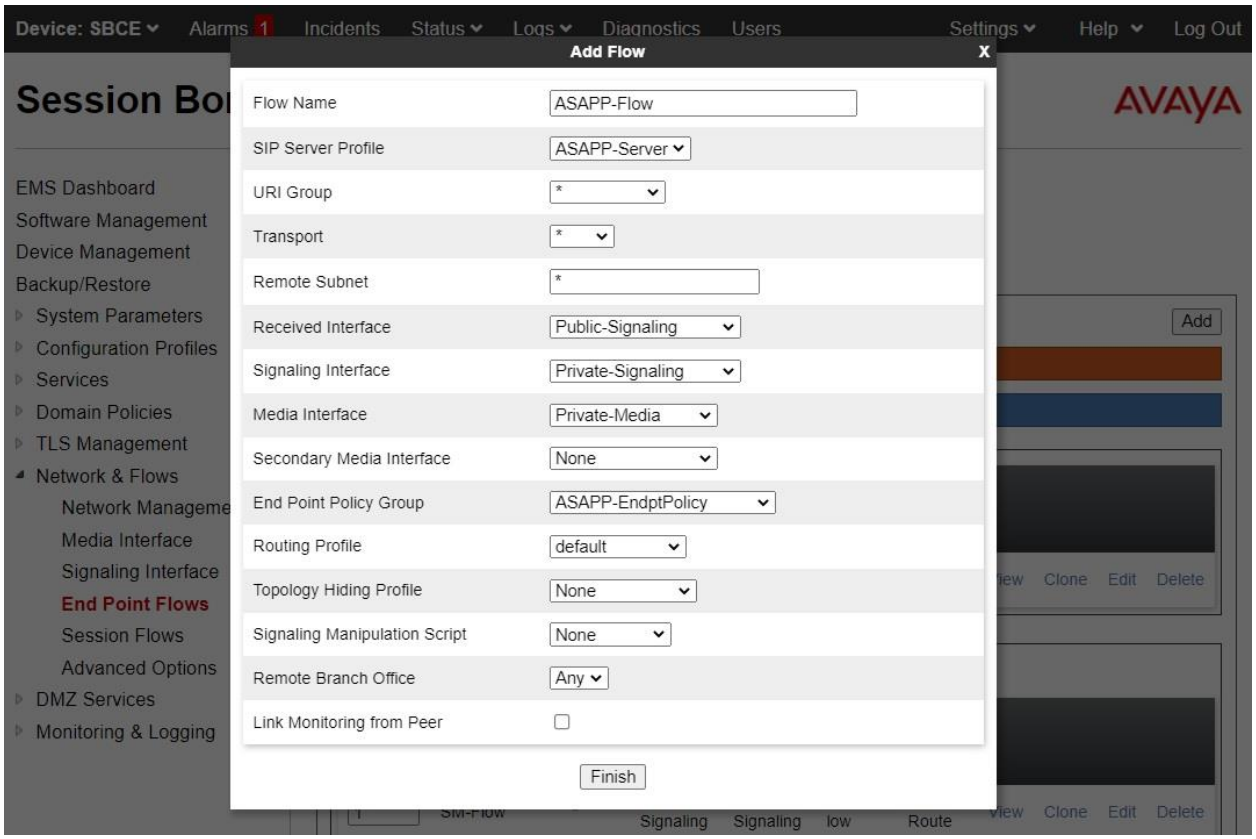
7.9. Administer End Point Flows

Select **Backup/Restore → Network & Flows → End Point Flows** from the left pane. Select the **Server Flows** tab and click **Add** to add a server flow for ASAPP.



The **Add Flow** pop-up screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Flow Name:** A descriptive name.
- **SIP Server Profile:** The ASAPP SIP server profile from **Section 7.2**.
- **Received Interface:** The external signaling interface in this case "Public-Signaling".
- **Signaling Interface:** The internal signaling interface in this case "Private-Signaling".
- **Media Interface:** The internal media interface in this case "Private-Media".
- **End Point Policy Group:** The ASAPP end point policy group from **Section 7.5**.



8. Configure ASAPP Voice Desk

The configuration of ASAPP on AWS is performed by the ASAPP Solution Architecture team and outside the scope of these Application Notes.

Prior to integration, the following set of information regarding Avaya resources were provided to ASAPP.

Entity	Value	Description
AES IP	10.64.101.239	IP address of Application Enablement Services
Tlink	See referenced section	Pertinent Tlink name from **Section 6.8**
CTI User	See referenced section	ASAPP user credentials from **Section 6.4**
CA Certificate	See referenced section	CA certificate from **Section 6.9**
Skill Group	61001, 61002	Skill group extensions from **Section 3**
Agent ID	65881, 65882	Agent IDs from **Section 3**

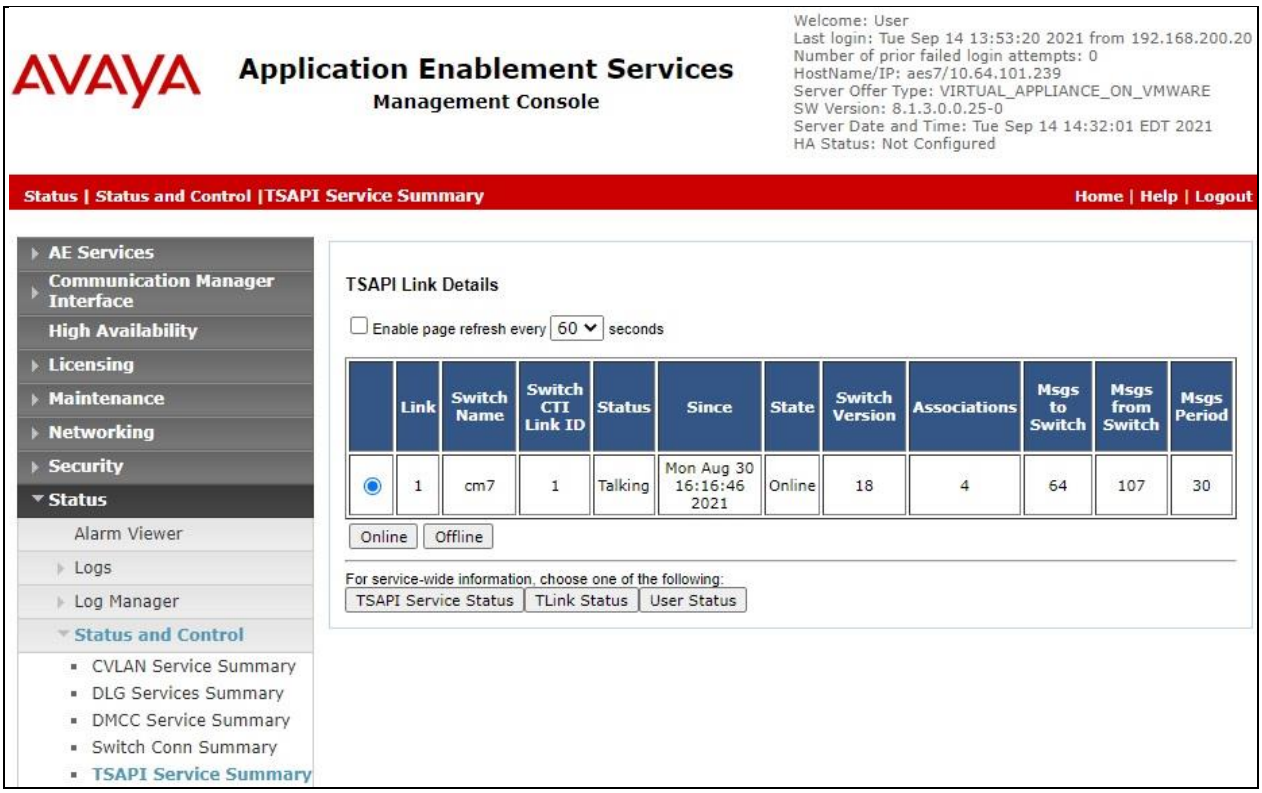
9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, SBCE, and ASAPP.

9.1. Verify TSAPI Connection

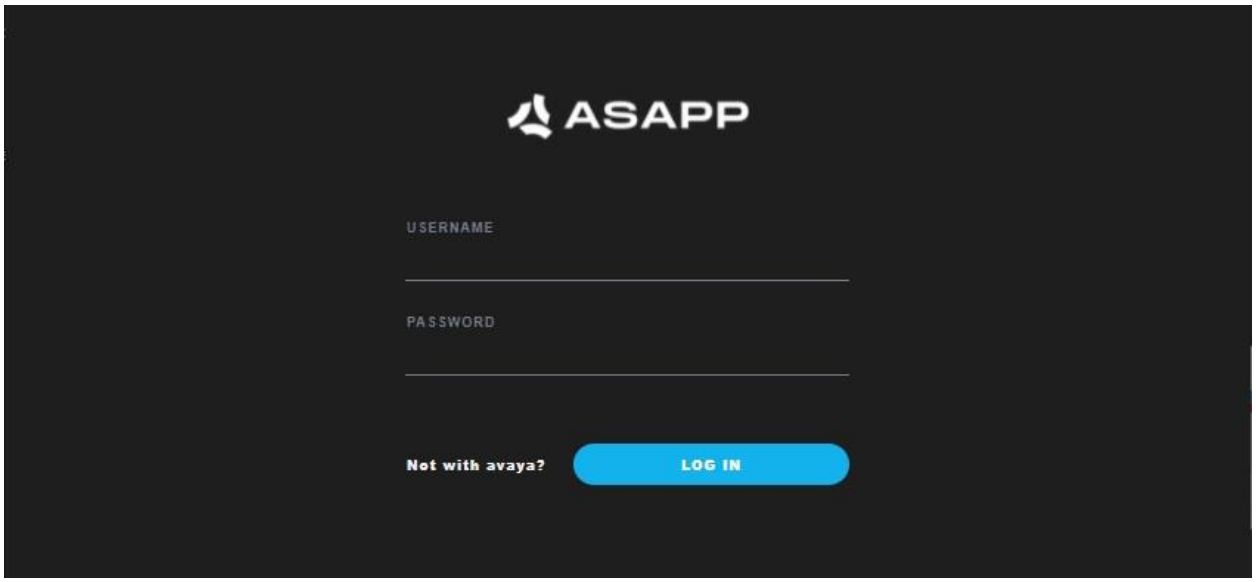
On Application Enablement Services, verify status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that **Status** is "**Talking**" for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3**, in this case "**4**".



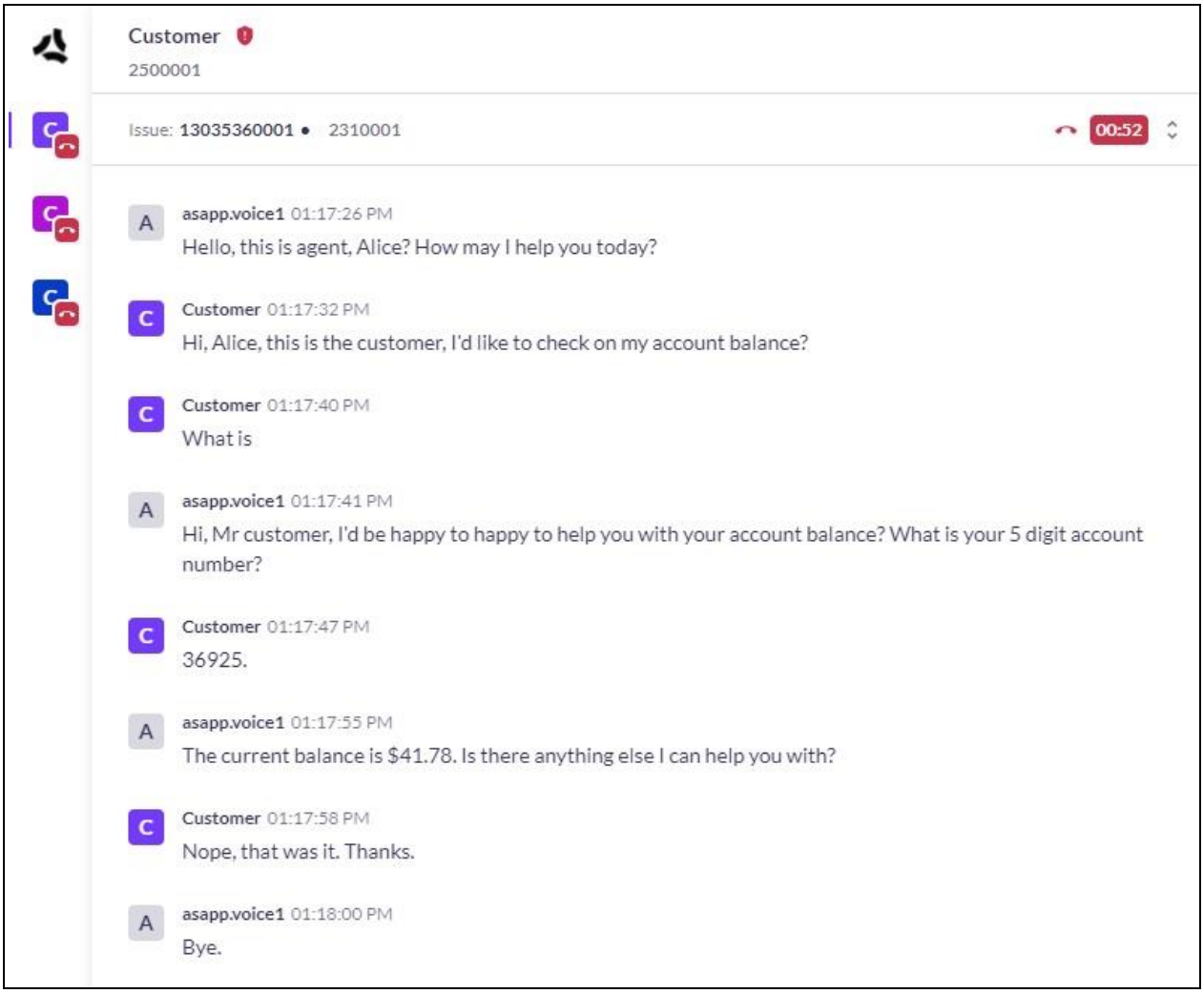
9.2. Verify SIPREC Transcription

From an agent PC, launch an Internet browser window and enter the URL provided by ASAPP. Log in with relevant user credentials provided by ASAPP.



The screen below is displayed next.

Establish an inbound ACD call with this agent. Verify that the screen is updated to reflect the dialed number in this case "**13035360001**", and that conversation text appears in the transcription area as shown below.



10. Conclusion

These Application Notes describe the configuration steps required for ASAPP Voice Desk 2.2 to successfully interoperate with Avaya Aura® Application Enablement Services 8.1 and Avaya Session Border Controller for Enterprise 8.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 7, October 2020, available at http://support.avaya.com.

2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020, available at http://support.avaya.com.

3. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 7, November 2020, available at http://support.avaya.com.

4. *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020, available at http://support.avaya.com.

5. *ASAPP Voice Integration Overview*, available from ASAPP Support.

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.